(19)日本国特許庁(JP)　　(12)公開特許公報(A)　　(11)公開番号
特開2022-162998
(P2022-162998A)
(43)公開日　令和4年10月25日(2022.10.25)

(51)国際特許分類			FI		
G06F	*21/34*	*(2013.01)*	G06F	21/34	
G06F	*21/64*	*(2013.01)*	G06F	21/64	
G06F	*21/60*	*(2013.01)*	G06F	21/60	320
G06F	*21/62*	*(2013.01)*	G06F	21/62	318

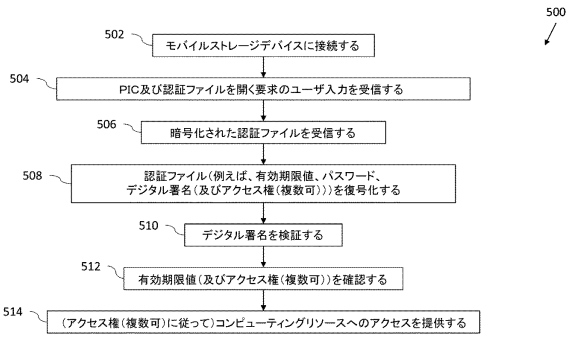
審査請求　未請求　請求項の数　43　　OL　外国語出願　（全34頁）

(21)出願番号　特願2022-65574(P2022-65574)
(22)出願日　令和4年4月12日(2022.4.12)
(31)優先権主張番号　63/174,269
(32)優先日　令和3年4月13日(2021.4.13)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　17/665,384
(32)優先日　令和4年2月4日(2022.2.4)
(33)優先権主張国・地域又は機関
米国(US)

(71)出願人　511099630
バイオセンス・ウエブスター・（イスラエル）・リミテッド
Ｂｉｏｓｅｎｓｅ Ｗｅｂｓｔｅｒ （Ｉｓｒａｅｌ）， Ｌｔｄ．
イスラエル国 ２０６６７１７ ヨークナム、ハトヌファ・ストリート ４
(74)代理人　100088605
弁理士　加藤 公延
(74)代理人　100130384
弁理士　大島 孝文
(72)発明者　エリヤフ・ラブナ
イスラエル国、２０６６７１７ ヨークナム、ハトヌファ・ストリート ４、ピー・オー・ボックス ２７５、バイオセ
最終頁に続く

(54)【発明の名称】　非接続デバイス内のユーザを認証する２要素認証

(57)【要約】　（修正有）
【課題】２要素認証及びモバイル（例えば、携帯型）記憶デバイスを使用して、ユーザを認証する方法及びシステムを提供する。
【解決手段】ユーザを認証する方法は、少なくともユーザ名及び有効期限値を含むログイン詳細の有効期限値及びデジタル署名を記憶するモバイルストレージデバイスに接続することと、モバイルストレージデバイスからデジタル署名及び有効期限値を受信することと、個人識別コードのユーザ入力を受信することと、有効期限値及びユーザ名に応答してデジタル署名を検証して、有効期限値及びユーザ名を認証することと、有効期限値が期限切れでないことを確認することと、有効期限値及びユーザ名が認証されていることと、有効期限値が期限切れでないことと、個人識別コードとに応答して、ユーザ名の下でログインされたコンピューティングリソースへのアクセスを提供することと、を含む。
【選択図】図５



【特許請求の範囲】
【請求項１】
ユーザを認証する方法であって、
ログイン詳細の有効期限値及びデジタル署名を記憶するモバイルストレージデバイスに接続することであって、前記ログイン詳細が、少なくともユーザ名及び前記有効期限値を含む、接続することと、
前記モバイルストレージデバイスから前記デジタル署名及び前記有効期限値を受信することと、
個人識別コードのユーザ入力を受信することと、
前記有効期限値及び前記ユーザ名に応答して前記デジタル署名を検証して、前記有効期限値及び前記ユーザ名を認証することと、
前記有効期限値が期限切れではないことを確認することと、
前記有効期限値及び前記ユーザ名が認証されていることと、前記有効期限値が期限切れではないことと、前記個人識別コードと、に応答して前記ユーザ名の下でログインされたコンピューティングリソースへのアクセスを提供することと、を含む方法。
【請求項２】
前記ログイン詳細が、少なくとも１つのアクセス権を含み、
前記検証することが、前記有効期限値、前記ユーザ名、及び前記少なくとも１つのアクセス権に応答して前記デジタル署名を検証して、前記有効期限値、前記ユーザ名、及び前記少なくとも１つのアクセス権を認証することを含み、
前記確認することが、前記少なくとも１つのアクセス権を確認して、機能へのアクセスが認証されているかどうかを検証することを含み、
前記アクセスを提供することが、検証された前記少なくとも１つのアクセス権に従って、前記コンピューティングリソースへのアクセスを提供することを含む、請求項１に記載の方法。
【請求項３】
前記モバイルストレージデバイスが、暗号化形式で前記有効期限値を記憶し、前記方法が、前記個人識別コードに応答して前記有効期限値を復号化することを更に含む、請求項１に記載の方法。
【請求項４】
前記モバイルストレージデバイスが、前記ユーザ名を暗号化形式で記憶し、前記方法が、前記個人識別コードに応答して前記ユーザ名を復号化することを更に含む、請求項３に記載の方法。
【請求項５】
前記モバイルストレージデバイスが、暗号化形式で前記デジタル署名を記憶し、前記方法が、前記個人識別コードに応答して前記デジタル署名を復号化することを更に含む、請求項１に記載の方法。
【請求項６】
前記個人識別コードに応答して前記有効期限値、前記ユーザ名、及び前記デジタル署名のうちの少なくとも１つを対称復号化することを更に含む、請求項１に記載の方法。
【請求項７】
前記デジタル署名が、公開鍵基盤の秘密鍵及び公開鍵にそれぞれ応答して生成及び検証される、請求項１に記載の方法。
【請求項８】
前記ユーザ名のユーザ入力を受信することと、
前記有効期限値、前記ユーザ名、及び前記個人識別コードに応答して前記デジタル署名を検証して、前記有効期限値、前記ユーザ名、及び前記個人識別コードを認証することと、を更に含む、請求項１に記載の方法。
【請求項９】
ウェブサーバを前記モバイルストレージデバイスに接続することと、

前記ウェブサーバによって前記ユーザ名、パスワード、及び前記個人識別コードのユーザ入力を受信することと、
前記ウェブサーバによって前記有効期限値を生成することと、
前記ログイン詳細の前記デジタル署名を生成することと、
前記パスワードを認証したことに応答して前記ログイン詳細の前記有効期限値及び前記デジタル署名を前記モバイルストレージデバイスに記憶することと、を更に含む、請求項１に記載の方法。
【請求項１０】
前記個人識別コードに応答して前記有効期限値を暗号化することを更に含み、前記記憶することが、暗号化された前記有効期限値を前記モバイルストレージデバイスに記憶することを含む、請求項９に記載の方法。
【請求項１１】
前記個人識別コードに応答して前記ユーザ名を暗号化することを更に含み、前記記憶することが、暗号化された前記ユーザ名を前記モバイルストレージデバイスに記憶することを含む、請求項１０に記載の方法。
【請求項１２】
前記個人識別コードに応答して前記デジタル署名を暗号化することを更に含み、前記記憶することが、暗号化された前記デジタル署名を前記モバイルストレージデバイスに記憶することを含む、請求項９に記載の方法。
【請求項１３】
前記ログイン詳細が、前記個人識別コードを含む、請求項９に記載の方法。
【請求項１４】
前記モバイルストレージデバイスが、ユーザ取り消しリストを記憶し、前記デジタル署名が、前記ログイン詳細及び前記ユーザ取り消しリストにデジタル署名し、前記方法が、
前記モバイルストレージデバイスから前記ユーザ取り消しリストを受信することと、
前記ユーザ取り消しリストに応答して前記デジタル署名を検証して、前記ユーザ取り消しリストを認証することと、
認証された前記ユーザ取り消しリストに応答して前記コンピューティングリソースへのアクセスを拒否することと、を更に含む、請求項１に記載の方法。
【請求項１５】
前記モバイルストレージデバイスが、前記ユーザ取り消しリストのバージョン識別情報を記憶し、前記方法が、認証された前記ユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証された前記ユーザ取り消しリストの前記バージョン識別情報が示すことに応答して、前記古いユーザ取り消しリストの使用を認証された前記ユーザ取り消しリストに置き換えることを更に含む、請求項１４に記載の方法。
【請求項１６】
前記デジタル署名が、公開鍵基盤の第１の秘密鍵及び第１の公開鍵にそれぞれ応答して生成及び検証され、
前記モバイルストレージデバイスが、第２の公開鍵を記憶し、前記デジタル署名が、前記ログイン詳細及び前記第２の公開鍵にデジタル署名し、前記方法が、
前記モバイルストレージデバイスから前記第２の公開鍵を受信することと、
前記第１の公開鍵に応答して前記デジタル署名を検証して、前記第２の公開鍵を認証することと、
前記第２の公開鍵が認証されていることに応答して前記第２の公開鍵で追加のデジタル署名を検証することと、を更に含む、請求項１に記載の方法。
【請求項１７】
前記モバイルストレージデバイスが、前記第１の公開鍵及び前記第２の公開鍵を含む新しい公開鍵リストと、前記新しい公開鍵リストのバージョン識別情報と、を記憶し、前記方法が、前記新しい公開鍵リストが古い公開鍵リストよりも新しいことを、前記新しい公開鍵リストの前記バージョン識別情報が示すことに応答して、前記古い公開鍵リストの使

用を前記新しい公開鍵リストに置き換えることを更に含む、請求項１６に記載の方法。
【請求項１８】
ユーザを認証する方法であって、
ユーザ取り消しリストと、ログイン詳細及び前記ユーザ取り消しリストのデジタル署名とを記憶する、モバイルストレージデバイスに接続することと、
前記モバイルストレージデバイスから前記デジタル署名及び前記ユーザ取り消しリストを受信することと、
前記ユーザ取り消しリスト及びログインデータに応答して前記デジタル署名を検証して、前記ログイン詳細に含まれる前記ユーザ取り消しリスト及び前記ログインデータを認証することと、
認証された前記ログインデータに応答してコンピューティングリソースへのアクセスを提供することと、
認証された前記ユーザ取り消しリストに応答して前記コンピューティングリソースへのアクセスを拒否することと、を含む、方法。
【請求項１９】
前記モバイルストレージデバイスが、前記ユーザ取り消しリストのバージョン識別情報を記憶し、前記方法が、認証された前記ユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証された前記ユーザ取り消しリストの前記バージョン識別情報が示すことに応答して、前記古いユーザ取り消しリストの使用を認証された前記ユーザ取り消しリストに置き換えることを更に含む、請求項１８に記載の方法。
【請求項２０】
ユーザを認証する方法であって、
第１の公開鍵、第２の公開鍵に応答して検証のための第１の秘密鍵に応答して生成されたデジタル署名を記憶するモバイルストレージデバイスに接続することであって、前記デジタル署名がログイン詳細及び前記第２の公開鍵にデジタル署名する、接続することと、
前記モバイルストレージデバイスから前記デジタル署名及び前記第２の公開鍵を受信することと、
前記第１の公開鍵に応答して前記デジタル署名を検証して、前記ログイン詳細に含まれる前記第２の公開鍵及びログインデータを認証することと、
認証された前記ログインデータに応答してコンピューティングリソースへのアクセスを提供することと、
前記第２の公開鍵が認証されていることに応答して前記第２の公開鍵で追加のデジタル署名を検証することと、を含む、方法。
【請求項２１】
前記モバイルストレージデバイスが、前記第１の公開鍵及び前記第２の公開鍵を含む新しい公開鍵リストと、前記新しい公開鍵リストのバージョン識別情報と、を記憶し、前記方法が、前記新しい公開鍵リストが古い公開鍵リストよりも新しいことを、前記新しい公開鍵リストの前記バージョン識別情報が示すことに応答して、前記古い公開鍵リストの使用を前記新しい公開鍵リストに置き換えることを更に含む、請求項２０に記載の方法。
【請求項２２】
処理デバイスを備えるユーザを認証するためのシステムであって、前記処理デバイスが、
ログイン詳細の有効期限値及びデジタル署名を記憶するモバイルストレージデバイスに接続するように構成されたデータインターフェースであって、前記ログイン詳細が、少なくともユーザ名及び前記有効期限値を含む、データインターフェースと、
ユーザ入力デバイスと、
処理回路であって、前記モバイルストレージデバイスから前記デジタル署名及び前記有効期限値を受信し、前記ユーザ入力デバイスを介して個人識別コードのユーザ入力を受信し、前記有効期限値及び前記ユーザ名に応答して前記デジタル署名を検証して、前記有効期限値及び前記ユーザ名を認証し、前記有効期限値が期限切れでないことを確認し、前記

有効期限値及び前記ユーザ名が認証されていることと、前記有効期限値が期限切れでないことと、前記個人識別コードと、に応答して前記ユーザ名の下でログインされたコンピューティングリソースへのアクセスを提供する、
ように構成された、処理回路と、
を備える、システム。
【請求項２３】
前記ログイン詳細が、少なくとも１つのアクセス権を含み、
前記処理回路が、
前記有効期限値、前記ユーザ名、及び前記少なくとも１つのアクセス権に応答して前記デジタル署名を検証して、前記有効期限値、前記ユーザ名、及び前記少なくとも１つのアクセス権を認証し、
前記少なくとも１つのアクセス権を確認して、機能へのアクセスが認証されているかどうかを検証し、
検証された前記少なくとも１つのアクセス権に従って、前記コンピューティングリソースへのアクセスを提供する
ように構成されている、請求項２２に記載のシステム。
【請求項２４】
前記モバイルストレージデバイスが、暗号化形式で前記有効期限値を記憶するように構成され、
前記処理回路が、前記個人識別コードに応答して前記有効期限値を復号化するように構成されている、請求項２２に記載のシステム。
【請求項２５】
前記モバイルストレージデバイスが、暗号化形式で前記ユーザ名を記憶するように構成され、
前記処理回路が、前記個人識別コードに応答して前記ユーザ名を復号化するように構成されている、請求項２４に記載のシステム。
【請求項２６】
前記モバイルストレージデバイスが、暗号化形式で前記デジタル署名を記憶するように構成され、
前記処理回路が、前記個人識別コードに応答して前記デジタル署名を復号化するように構成されている、請求項２２に記載のシステム。
【請求項２７】
前記処理回路が、前記個人識別コードに応答して前記有効期限値、前記ユーザ名、及び前記デジタル署名のうちの少なくとも１つを対称復号化するように構成されている、請求項２２に記載のシステム。
【請求項２８】
前記処理回路が、公開鍵基盤の公開鍵に応答して前記デジタル署名を検証するように構成されている、請求項２２に記載のシステム。
【請求項２９】
前記処理回路が、
前記ユーザ名のユーザ入力を受信し、
前記有効期限値、前記ユーザ名、及び前記個人識別コードに応答して前記デジタル署名を検証して、前記有効期限値、前記ユーザ名、及び前記個人識別コードを認証する、
ように構成されている、請求項２２に記載のシステム。
【請求項３０】
サーバを更に備え、前記サーバが、
前記モバイルストレージデバイスに接続し、
前記ユーザ名、パスワード、及び前記個人識別コードのユーザ入力を受信し、
前記有効期限値を生成し、
前記ログイン詳細の前記デジタル署名を生成し、

前記パスワードを認証したことに応答して、前記ログイン詳細の前記有効期限値及び前記デジタル署名を前記モバイルストレージデバイスに記憶する、
ように構成されている、請求項２２に記載のシステム。
【請求項３１】
前記サーバが、公開鍵基盤の秘密鍵に応答して前記デジタル署名を生成するように構成されている、請求項３０に記載のシステム。
【請求項３２】
前記サーバが、
前記個人識別コードに応答して前記有効期限値を暗号化し、
暗号化された前記有効期限値を前記モバイルストレージデバイスに記憶する、
ように構成されている、請求項３０に記載のシステム。
【請求項３３】
前記サーバが、
前記個人識別コードに応答して前記ユーザ名を暗号化し、
暗号化された前記ユーザ名を前記モバイルストレージデバイスに記憶する、
ように構成されている、請求項３２に記載のシステム。
【請求項３４】
前記サーバが、
前記個人識別コードに応答して前記デジタル署名を暗号化し、
暗号化された前記デジタル署名を前記モバイルストレージデバイスに記憶する、
ように構成されている、請求項３０に記載のシステム。
【請求項３５】
前記ログイン詳細が、前記個人識別コードを含む、請求項３０に記載のシステム。
【請求項３６】
前記モバイルストレージデバイスが、ユーザ取り消しリストを記憶し、前記デジタル署名が、前記ログイン詳細及び前記ユーザ取り消しリストにデジタル署名し、
前記処理回路が、
前記モバイルストレージデバイスから前記ユーザ取り消しリストを受信し、
前記ユーザ取り消しリストに応答して前記デジタル署名を検証して、前記ユーザ取り消しリストを認証し、
認証された前記ユーザ取り消しリストに応答して前記コンピューティングリソースへのアクセスを拒否する、
ように構成されている、請求項２２に記載のシステム。
【請求項３７】
前記モバイルストレージデバイスが、前記ユーザ取り消しリストのバージョン識別情報を記憶し、
前記処理回路が、認証された前記ユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証された前記ユーザ取り消しリストの前記バージョン識別情報が示すことに応答して、前記古いユーザ取り消しリストの使用を認証された前記ユーザ取り消しリストに置き換えるように構成されている、請求項３６に記載のシステム。
【請求項３８】
前記デジタル署名が、公開鍵基盤の第１の秘密鍵及び第１の公開鍵にそれぞれ応答して生成及び検証され、
前記モバイルストレージデバイスが、第２の公開鍵を記憶し、前記デジタル署名が、前記ログイン詳細及び前記第２の公開鍵にデジタル署名し、
前記処理回路が、
前記モバイルストレージデバイスから前記第２の公開鍵を受信し、
前記第１の公開鍵に応答して前記デジタル署名を検証して、前記第２の公開鍵を認証し、
前記第２の公開鍵が認証されていることに応答して前記第２の公開鍵で追加のデジタル

署名を検証する
ように構成されている、請求項２２に記載のシステム。
【請求項３９】
前記モバイルストレージデバイスが、前記第１の公開鍵及び前記第２の公開鍵を含む新しい公開鍵リストと、前記新しい公開鍵リストのバージョン識別情報と、を記憶し、
前記処理回路が、前記新しい公開鍵リストが古い公開鍵リストより新しいことを、前記新しい公開鍵リストの前記バージョン識別情報が示すことに応答して、前記古い公開鍵リストの使用を前記新しい公開鍵リストに置き換えるように構成されている、請求項３８に記載のシステム。
【請求項４０】
ユーザを認証するためのシステムであって、
ユーザ取り消しリストと、ログイン詳細及び前記ユーザ取り消しリストにデジタル署名するデジタル署名と、を記憶するモバイルストレージデバイスに接続するように構成されたデータインターフェースと、
処理回路であって、
前記モバイルストレージデバイスから前記デジタル署名及び前記ユーザ取り消しリストを受信し、
前記ユーザ取り消しリスト及びログインデータに応答して前記デジタル署名を検証して、前記ログイン詳細に含まれる前記ユーザ取り消しリスト及び前記ログインデータを認証し、
認証された前記ログインデータに応答してコンピューティングリソースへのアクセスを提供し、
認証された前記ユーザ取り消しリストに応答して前記コンピューティングリソースへのアクセスを拒否する
ように構成されている、処理回路と、
を備えるシステム。
【請求項４１】
前記モバイルストレージデバイスが、前記ユーザ取り消しリストのバージョン識別情報を記憶し、
前記処理回路が、認証された前記ユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証された前記ユーザ取り消しリストの前記バージョン識別情報が示すことに応答して、前記古いユーザ取り消しリストの使用を認証された前記ユーザ取り消しリストに置き換えるように構成されている、請求項４０に記載のシステム。
【請求項４２】
ユーザを認証するためのシステムであって、
第１の公開鍵、第２の公開鍵に応答して検証のための第１の秘密鍵に応答して生成されたデジタル署名を記憶するモバイルストレージデバイスに接続するように構成されたデータインターフェースであって、前記デジタル署名がログイン詳細及び前記第２の公開鍵にデジタル署名する、データインターフェースと、
処理回路であって、
前記モバイルストレージデバイスから前記デジタル署名及び前記第２の公開鍵を受信し、
前記第１の公開鍵に応答して前記デジタル署名を検証して、前記ログイン詳細に含まれる前記第２の公開鍵及びログインデータを認証し、
認証された前記ログインデータに応答してコンピューティングリソースへのアクセスを提供し、
前記第２の公開鍵が認証されていることに応答して前記第２の公開鍵で追加のデジタル署名を検証する
ように構成されている、処理回路と、
を備えるシステム。

【請求項４３】
前記モバイルストレージデバイスが、前記第１の公開鍵及び前記第２の公開鍵を含む新しい公開鍵リストと、前記新しい公開鍵リストのバージョン識別情報と、を記憶し、
前記処理回路が、前記新しい公開鍵リストが古い公開鍵リストより新しいことを、前記新しい公開鍵リストの前記バージョン識別情報が示すことに応答して、前記古い公開鍵リストの使用を前記新しい公開鍵リストに置き換えるように構成されている、請求項４２に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、コンピューティングデバイスに関し、特に、限定はしないが、ユーザ認証に関する。
【背景技術】
【０００２】
技術者は、医療センターなどの異なる場所を訪れて、ローカルデバイス、例えば、カリフォルニア州アーバインのＢｉｏｓｅｎｓｅ Ｗｅｂｓｔｅｒ Ｉｎｃ．のＣＡＲＴＯ（登録商標）３ Ｓｙｓｔｅｍなどの医療システム上でメンテナンスタスクを実行することがある。ローカルデバイスは、インターネットに接続されない場合があり、このことは、技術者がローカルデバイスにアクセスし、どの技術者がどのローカルデバイスにログインしたかを追跡するという課題を提起する。
【０００３】
Ｇａｎｔｍａｎらの米国特許第８，０４６，５８７号は、オフラインのリソースが制限されたモバイルデバイスへ認証されたアクセスを付与する方法について記載している。公開－秘密鍵ペアは、サービスプロバイダによって生成され、公開鍵は、ユーザ名及び（場合によっては）アクセス権限にデジタル署名して、技術者のパスワードを取得するために使用される。公開鍵は、モバイルデバイスに安全に配布される。オフラインのとき、モバイルデバイスは、技術者によってモバイルデバイスの制限された機能へのアクセスを認証し得る。技術者は、ユーザ名、アクセス権限、及びパスワードをモバイルデバイスに提供する。次いで、モバイルデバイスは、公開鍵、ユーザ名、及びアクセス権限を使用して、パスワードを検証する。古いユーザ名及びパスワードを無効にするために、サービスプロバイダは、公開－秘密鍵ペアを新しい公開－秘密鍵ペアに置き換える。
【０００４】
ＢａｒｔｕｃｃｉらのＰＣＴ公開第ＷＯ２０１３／１２３４５３号は、携帯型電子メモリデバイス（例えば、ＵＳＢフラッシュドライブ）について記載している。例示的な態様は、キーパッド、暗号化ハードウェア、及び特別なドライバを受信システムにインストールする必要なく、遠隔コンピューティングシステムのための認証ツールを暗号化、復号化、又は機能させる能力を有する携帯型電子メモリデバイスを含む。
【０００５】
Ｃｏｒｒｉｏｎの米国特許第９，１１８，６６２号は、分散型ログオンサービスをオフラインコンピューティングデバイスに拡張するための方法及びシステムを記載しており、オフラインコンピューティングデバイス上で、ワンタイムパスワード（ＯＴＰ）、ノンス、及び一意の識別子を暗号化して認証要求メッセージを生成することを含む。モバイルデバイスをプロキシとして使用して、認証のために、認証要求メッセージをアクセス制御サーバに転送する。認証応答メッセージを復号化して、ノンスを取得する。ノンスを再暗号化して、認証応答メッセージを生成する。モバイルデバイスをプロキシとして使用して、認証応答メッセージをオフラインコンピューティングデバイスに転送する。認証応答メッセージを復号化して、ノンスを取得する。認証応答メッセージから取得されたノンスを元のノンスと比較する。コンピューティングデバイスは、認証応答メッセージから取得されたノンスを元のノンスと比較する結果としてアクセスを許可又は拒否する。
【０００６】

Ｂｏｋａｒｅらの米国特許第１０，３２６，７３３号は、複数のデバイスの単一のサインオンを容易にするためのコンピュータ実装方法を記載しており、この方法は、（１）ユーザアカウントのログインセッションを確立することと、（２）ログインセッションを確立することに応答して、ユーザアカウントに関連付けられたデバイスに、ユーザアカウントのセッショントークンを提供することと、（３）少なくとも１つのクライアントから、ユーザアカウントと関連付けられたリソースにアクセスする要求を受信することと、（４）関連付けられたデバイスがユーザアカウントのセッショントークンを保有していると判定することと、（５）関連付けられたデバイスがセッショントークンを保有していると判定したことに応答して、クライアントに、ユーザアカウントと関連付けられたリソースへのアクセスを提供することと、を含む。

【０００７】

Ａａｂｖｅらの米国特許公開第２０１５／０２２０９１７号は、限定的な使用証明書を使用してトークンを検証するための方法、デバイス、及びシステムを記載している。例えば、ユーザデバイスは、トークン要求をトークンプロバイダコンピュータに送信し、それに応答してトークン及びトークンに関連付けられたトークン証明書を受信することができる。トークン証明書は、例えば、トークンのハッシュと、トークンプロバイダコンピュータ又は別の信頼できるエンティティによるデジタル署名とを含んでもよい。ユーザデバイスは、トークン及びトークン証明書をアクセスデバイスに提供することができる。アクセスデバイスは、トークン証明書を使用してトークンを検証し、デジタル署名を使用してトークン証明書を検証することができる。場合によっては、トークン及びトークン証明書はオフラインで検証され得る。次に、アクセスデバイスは、トークンを使用してトランザクションを行うことができる。

【０００８】

Ｊｅｖａｎｓの米国特許第８，３２１，９５３号は、ユーザからオフラインでユーザコードを受信して、記憶されたデータへのアクセスを許可するように構成されたユーザインターフェースと、ユーザコードに少なくとも部分的に基づいて、記憶されたデータへのアクセスを認証して、記憶されたデータへのアクセスを提供するように構成された回路と、記憶されたデータを記憶するように構成されたストレージシステムと、を備える保護データストレージへのアクセスを認証するシステムを記載している。

【０００９】

セキュリティアサーションマークアップ言語（ＳＡＭＬ）は、当事者間、特にアイデンティティプロバイダとサービスプロバイダとの間で、認証及び認証データを交換するためのオープン標準である。ＳＡＭＬは、ｅｎ．ｗｉｋｉｐｅｄｉａ．ｏｒｇ／ｗｉｋｉ／Ｓｅｃｕｒｉｔｙ＿Ａｓｓｅｒｔｉｏｎ＿Ｍａｒｋｕｐ＿Ｌａｎｇｕａｇｅにより詳細に記載されている。

【図面の簡単な説明】

【００１０】

本開示は、添付の図面と併せて、以下の詳細な説明から理解されよう。

【図１】本開示の例示的な態様により構築され、動作する２要素認証システムの部分描写図、部分ブロック図である。

【図２】図１のシステムにおいて使用するための認証ファイルを生成する方法における工程を含むフローチャートである。

【図３】ユーザによって使用されて、図１のシステムの認証ファイルを生成するユーザインターフェース画面の概略図である。

【図４】図１のシステムと共に使用するための認証ファイルがその中に記憶されたモバイルストレージデバイスの概略図である。

【図５】認証ファイルを検証して、図１のシステム内のコンピューティングリソースへのアクセスを提供する方法における工程を含むフローチャートである。

【図６】ユーザによって使用されて、図１のシステムのコンピューティングリソースにログインするユーザインターフェース画面の概略図である。

【図７】図１のシステムにおいて使用するための認証ファイルを生成する別の方法における工程を含むフローチャートである。
【図８】認証ファイルを検証して、図１のシステム内のコンピューティングリソースへのアクセスを提供する別の方法における工程を含むフローチャートである。
【図９】図１のシステムと共に使用するためのより多くのデータを有する認証ファイルがその中に記憶された図４のモバイルストレージデバイスの概略図である。
【図１０】認証ファイルを検証して、図１のシステム内のコンピューティングリソースへのアクセスを提供して、ユーザ取り消しリスト及び／又は公開鍵リストを置き換える別の方法における工程を含むフローチャートである。
【発明を実施するための形態】
【００１１】
概論
前述したように、技術者は、医療センターなどの様々な場所を訪れて、ローカルデバイス、例えば、カリフォルニア州アーバインのＢｉｏｓｅｎｓｅ Ｗｅｂｓｔｅｒ Ｉｎｃ．のＣＡＲＴＯ（登録商標）３ Ｓｙｓｔｅｍなどの医療システム上でメンテナンスタスクを実行することがある。
【００１２】
ローカルデバイスは、インターネットに、又は任意の適切なネットワークを介して接続され得ないことがあり、このことは、技術者がローカルデバイスにアクセスし、どの技術者がどのローカルデバイスにログインしたかを追跡する課題を提起する。
【００１３】
１つの解決策は、全てのローカルデバイス上の全ての技術者に対して同じハードコードされたパスワードを使用することである。しかしながら、これは、低レベルのセキュリティを提供し、個々の技術者を一意に識別しない。また、技術者がローカルデバイスを保守するためにもはや雇用されていない場合でも、技術者は依然としてローカルデバイスにアクセスできる。
【００１４】
本開示の例示的な態様は、２要素認証及びモバイル（例えば、携帯型）記憶デバイスを使用して、認証ファイルを記憶し、異なる非接続処理デバイスでコンピューティングリソースを使用するために個々のユーザ（例えば、技術者）を認証することによって、上記の問題を解決する。
【００１５】
技術者は、オンライン認証アプリケーション（例えば、ウェブアプリケーション）から認証ファイルを受信する。次いで、認証ファイルは、フラッシュディスク、ＣＤ、ＤＶＤ、又はＳＤカードなどのモバイルストレージデバイスに記憶される。認証ファイルにより、技術者は、異なる非接続処理デバイスのコンピューティングリソースにアクセスすることができる。次いで、技術者は、モバイルストレージデバイスを非接続処理デバイスのうちの１つに取り込み、モバイルストレージデバイスに記憶された認証ファイルを検証することに応答して処理デバイスへのアクセスが提供される。ここで、認証ファイルを提供し、認証ファイルを使用するプロセスをより詳細に説明する。
【００１６】
技術者は、サーバ上で実行されるオンライン認証アプリケーション（例えば、ウェブサーバによってホストされるウェブアプリケーション）、又はネットワーク（例えば、インターネット又はイントラネット）内の複数の場所からアクセスされ得る任意の適切なアプリケーションにログインする。オンラインアプリケーションへのログインは、技術者が、アプリケーションによって認証されたユーザ名及びパスワードを供給することを含み得る。ユーザ名及びパスワードが認証された後、認証アプリケーションは、数字及び／又は文字及び／又は記号を含み得る個人識別コード（ＰＩＣ）を入力するように技術者に促す。ＰＩＣは、典型的には、技術者によって選択される。あるいは、ＰＩＣは、認証アプリケーションによって提供され得る。認証アプリケーションは、任意の好適な値であり得る有

効期限値（例えば、有効期限日）を生成する。例えば、有効期限値は、現在の時刻／日の後の所与の数の時間、日、週、又は月の場合であってもよい。認証アプリケーションは、有効期限値及びユーザ名を含むログイン詳細のデジタル署名を生成する。ログイン詳細はまた、技術者がアクセスを許可される機能、例えば、ユーザの許可、アクセスレベル、又は種類を決定する１つ以上のアクセス権を含み得る。デジタル署名は、典型的には、（例えば、秘密鍵を含む証明書に基づいて）技術者の雇用者などの認証団体の秘密鍵を使用する非対称暗号化を使用して生成される。次いで、認証アプリケーションは、（例えば、ＰＩＣに基づく鍵を使用する対称暗号化を使用して）デジタル署名、有効期限値、及びユーザ名を暗号化する。デジタル署名、有効期限値、及びユーザ名は、単一の暗号化項目として、又は別個の暗号化項目として暗号化され得る。次に、認証アプリケーションは、暗号化されたデジタル署名、有効期限値、及びユーザ名（例えば、暗号化された認証ファイル）を、技術者のモバイルストレージデバイス内の認証ファイルに記憶する。いくつかの例示的な態様では、有効期限値は、平文で（すなわち、暗号化されずに）残されて、モバイルストレージデバイス内に平文で記憶され得る。

【００１７】

いったん認証ファイル又は関連値がモバイルストレージデバイスに記憶されると、技術者は、非接続処理デバイスのいずれかにモバイルストレージデバイスを取り込み得る。選択された非接続処理デバイスのうちの１つでは、技術者は、その処理デバイス上で実行される認証アプリケーションによってレンダリングされたユーザインターフェース画面内にＰＩＣを入力し、技術者は、モバイルストレージデバイスに記憶された認証ファイルの開くことを要求する。認証アプリケーションは、認証ファイルを受信し、（例えば、ＰＩＣに基づくキーに応答して対称復号化を使用して）認証ファイルを復号化する。次いで、認証アプリケーションは、認証ファイルに記憶されたユーザ名及び有効期限値に応答してデジタル署名を検証する。デジタル署名は、典型的には、（例えば、公開鍵を含む証明書に基づいて）技術者の雇用者などの認証団体の公開鍵を使用する非対称暗号化を使用して検証される。有効期限値が確認されて、期限切れでないことを保証する。任意選択的に、ログイン詳細に含まれるアクセス権（複数可）（例えば、ユーザの許可、アクセスレベル、又は種類）が確認されて、技術者が要求された機能にアクセスすることを認証されているかどうか、又は検証されたアクセス権（複数可）に基づいて機能を許可及び／又は解除するかを検証する。認証アプリケーションは、デジタル署名及び有効期限値を認証したことに応答して、ユーザ名の下でログインされたコンピューティングリソースへの技術者アクセスを提供する。

【００１８】

上記のようにして、技術者には、異なる非接続処理デバイスでのコンピューティングリソースへの時刻／日付が制限されたアクセスが提供され得る。アクセスは、デジタル署名及びＰＩＣを使用して保護されることによって、２要素セキュリティを提供して、（ＰＩＣに基づいて）個々の技術者のコンピューティングリソースの使用を制限し、（ユーザ名に基づいて）各技術者がコンピューティングリソースにログインした各技術者を識別する。

【００１９】

いくつかの例示的な態様では、認証アプリケーションは、有効期限値、ユーザ名、及びＰＩＣの署名を含むように認証ファイルを生成する。これらの例示的な態様では、有効期限値は、モバイルストレージデバイスに平文で記憶され得、ＰＩＣは、一般に、暗号化鍵を形成するために使用されない。これらの例示的な態様では、非接続処理デバイスのうちの１つにおいて、技術者は、（ユーザ名がモバイルストレージデバイスに記憶されていない場合）ＰＩＣ及びユーザ名を入力するように促される。次いで、認証アプリケーションは、デジタル署名を検証する（それにより、ユーザ名、有効期限値、及びＰＩＣを認証し、有効期限値を確認する）。認証アプリケーションは、デジタル署名及び有効期限値を認証したことに応答して、ユーザ名の下でログインされたコンピューティングリソースへの技術者アクセスを提供する。

【００２０】
いくつかの例示的な態様では、認証ファイルはまた、ユーザ取り消しリストを含み得る。ユーザ取り消しリストは、取り消されたが期限切れではない認証ファイル又は取り消されたが期限切れではない認証ファイルのユーザをリスト化し得る。例えば、Ｅｖｅ及びＭａｌｌｏｒｙなどの技術者は退職しているが、彼らのモバイルストレージデバイス上の認証ファイルは、更に数週間、依然として有効である。したがって、Ｅｖｅ及びＭａｌｌｏｒｙは、各自のモバイルストレージデバイスを使用してコンピューティングリソースに不正にアクセスすることができる。現在雇用されている技術者のＡｌｉｃｅが、この期間中に新しい認証ファイルを要求する場合、Ｅｖｅ及びＭａｌｌｏｒｙの両方をリスト化するユーザ取り消しリスト（例えば、彼らのために生成された認証ファイルの詳細などの電子メール、ユーザ名、及び／又は他の識別詳細など）を新しい認証ファイルに追加することができ、それにより、Ａｌｉｃｅが異なるデバイスにログインするときにユーザ取り消しリストをそれぞれのデバイスにコピーすることができるため、ＥｖｅとＭａｌｌｏｒｙが彼らのデバイスにログインしようとすると、ＥｖｅとＭａｌｌｏｒｙはユーザ取り消しリストに基づいてブロックされる。したがって、認証ファイルを要求し、認証ファイルに基づいてデバイスにログインするプロセスの結果として、ユーザ取り消しリストが、ログインされているデバイスにコピーされる。ユーザ取り消しリストは、認証ファイルに含まれ、デジタル署名はまた、ユーザがデバイスにログインするときにユーザ取り消しリストの真正性を確認することができるように、ユーザ取り消しリストに署名する。

【００２１】
いくつかの例示的な態様では、ユーザ取り消しリストは、バージョン識別情報（ＩＤ）（例えば、バージョン番号及び／又は日付）を含み得る。バージョン識別情報は、リストを認証するデバイスによって使用されて、以前に記憶されたユーザ取り消しリストが、ログインしている現在のユーザの認証ファイルに含まれるユーザ取り消しリストによって置き換えられるべきかどうかを判定することができる。例えば、Ａｌｉｃｅが医療デバイスにログインすると、医療デバイスは、Ａｌｉｃｅの認証ファイルに含まれるユーザ取り消しリストのバージョン識別情報（例えば、日付）が、医療デバイスのメモリに記憶されたユーザ取り消しリストのバージョン識別情報よりも新しいかどうかを確認する。実際に新しい場合、医療デバイスは、記憶されたユーザ取り消しリストを、Ａｌｉｃｅの認証ファイルで発見されるリストに置き換える。

【００２２】
異なる非接続処理デバイスにおける各コンピューティングリソースに、署名を検証するための少なくとも１つの公開鍵などがロードされているが、公開鍵は期限切れであるか、又は秘密－公開鍵ペアが危険にさらされている場合がある。したがって、１つ以上の予備の秘密－公開鍵ペアを生成し、デバイス上に少なくとも１つの予備公開鍵をロードすることが重要である。しかしながら、これは、デバイスがネットワークを介して接続され得ないことがあるため、問題となる。新しい秘密鍵は、その公開鍵の片割れが現場内の全てのデバイスに分配されるまで使用することができないことに留意されたい。移行を容易にするために、以下でより詳細に説明するように、認証ファイルを使用して、予備公開鍵（複数可）を分配することができる。

【００２３】
したがって、いくつかの例示的な態様では、認証ファイルは、少なくとも１つの予備公開鍵も含み得る。例えば、Ａｌｉｃｅが、新しい認証ファイルを要求する場合、１つ以上の予備公開鍵を新しい認証ファイルに追加することができ、それにより、Ａｌｉｃｅが異なるデバイスにログインするとき、予備公開鍵（複数可）は、後で使用するためにそれぞれのデバイスにコピーされ得る。したがって、認証ファイルを要求し、認証ファイルに基づいてデバイスにログインするプロセスの結果として、予備公開鍵（複数可）がそのデバイスにコピーされる。予備公開鍵（複数可）は、認証ファイルに含まれ得、デジタル署名はまた、ユーザがデバイスにログインするときに予備公開鍵（複数可）の真正性を確認することができるように、予備公開鍵（複数可）に署名し得る。

【００２４】
いくつかの例示的な態様では、予備公開鍵（複数可）が、認証ファイル内の公開鍵リストに記憶され得る。公開鍵リストはまた、システムによって現在使用されている公開鍵を含み得る。公開鍵リストは、バージョン識別情報（ＩＤ）（例えば、バージョン番号及び／又は日付）を含み得る。バージョン識別情報は、デバイスによって使用されて、以前に記憶された公開鍵リストが、ログインしている現在のユーザの認証ファイルに含まれる公開鍵リストによって置き換えられるべきかどうかを判定することができる。例えば、Ａｌｉｃｅが医療デバイスにログインすると、医療デバイスは、Ａｌｉｃｅの認証ファイルに含まれる公開鍵リストのバージョン識別情報（例えば、日付）が、医療デバイスのメモリに記憶された公開鍵リストのバージョン識別情報よりも新しいかどうかを確認する。実際に新しい場合、医療デバイスは、記憶された公開鍵リストを、Ａｌｉｃｅの認証ファイルで発見されるリストに置き換える。次いで、新しい公開鍵リスト内の公開鍵がデバイスによって使用されて、デバイスに提示されたデジタル署名を確認することができる。
【００２５】
いったん全ての非接続デバイスが新しい公開鍵（複数可）を学習すると、新しい認証ファイルが新しい公開鍵の秘密鍵で署名され得る。その後、認証ファイルに記憶された公開鍵リストは、古い公開鍵を含む必要はなく、最終的には、全ての非接続デバイスは、公開鍵リストがそれらのデバイスにおいて置き換えられるときに古い公開鍵を忘れる。
【００２６】
本開示は、「技術者」という用語は単なる例として使用する。「技術者」という用語は、単に技術者としての役割を果たす人ではなく、任意の好適なユーザの動作を説明するものとして理解されるべきである。
【００２７】
システムの説明
ここで、本開示の典型的な実施形態に基づいて構築され、動作する２要素認証システム１０の部分描写図、部分ブロック図である図１を参照する。
【００２８】
２要素認証システム１０は、技術者１２又は任意の適切なユーザを認証して、異なる非接続処理デバイス１６（簡略化のために１つのみが示されている）の非接続コンピューティングリソース１４（簡略化のために１つのみが示される）を使用するように構成される。
【００２９】
２要素認証システム１０は、任意の適切なネットワーク２０（例えば、インターネット）を介してサーバ１８（例えば、ウェブサーバ）上で実行されるオンライン認証アプリケーション（例えば、ウェブアプリケーション）を含む。技術者１２は、モバイルストレージデバイス２２（例えば、フラッシュディスク、ＣＤ、ＤＶＤ、又はＳＤカード）をコンピューティングデバイス２４（例えば、パーソナルコンピュータ、ラップトップコンピュータ、携帯電話、又はタブレットコンピューティングデバイス）に接続し、コンピューティングデバイスは、ネットワーク２０を介してサーバ１８に接続される。技術者１２は、ユーザ入力デバイス２６（例えば、キーボード及び／又はマウス、又はタッチスクリーン）を介して、ユーザ名、パスワード、及び個人識別コード（ＰＩＣ）を入力する。認証アプリケーションは、図２～図４を参照してより詳細に説明されるように、ユーザ名、パスワード、及びＰＩＣを処理し、モバイルストレージデバイス２２に記憶するための認証ファイル２８を提供する。同様に、他の技術者は、個人用に設定された認証ファイルを受信することができる。
【００３０】
２要素認証システム１０はまた、図５及び図６を参照してより詳細に説明されるように、認証ファイルを認証するために、非接続処理デバイス１６のそれぞれのデバイスで実行される認証アプリケーションを含む。各処理デバイス１６は、（ログイン詳細（例えば、有効期限値、ユーザ名、及び任意選択的に１つ以上のアクセス権、例えば、ユーザの許可

、アクセスレベル、又は種類）、及び典型的には暗号化形式のログイン詳細のデジタル署名を記憶する）モバイルストレージデバイス２２に接続するように構成されたデータインターフェース３０を含み得る。各処理デバイス１６は、ユーザ入力デバイス３２及び処理回路３４を含み得る。

【００３１】

実際には、コンピューティングデバイス２４と処理回路３４の機能のうちの一部又は全てが、単一の物理的な構成要素内に組み合わされ得るか、又は、代替的に、複数の物理的な構成要素を使用して実装され得る。これらの物理的構成要素は、ハードワイヤード装置若しくはプログラマブル装置、又はこれら２つの組み合わせを備え得る。いくつかの典型的な実施形態では、コンピューティングデバイス２４と処理回路３４の機能のうちの少なくともいくつかは、好適なソフトウェアの制御下にあるプログラム可能なプロセッサによって実行されてもよい。このソフトウェアは、例えば、ネットワークを介して電子的形態で装置にダウンロードされ得る。代替的に又は追加的に、このソフトウェアは、光学的メモリ、磁気的メモリ又は電子的メモリなどの有形の非一時的なコンピュータ可読媒体に記憶され得る。

【００３２】

ここで、図１のシステム１０において使用するための認証ファイル２８を生成する方法における工程を含むフローチャート２００である図２を参照する。図１も参照されたい。

【００３３】

技術者１２は、モバイルストレージデバイス２２をコンピューティングデバイス２４と動作可能に接続する。例えば、技術者１２は、モバイルストレージデバイス２２をコンピューティングデバイス２４のデータインターフェースに挿入する。サーバ１８上で実行される認証アプリケーションは、モバイルストレージデバイス２２に接続するように構成される（ブロック２０２）。

【００３４】

サーバ１８上で実行される認証アプリケーションは、技術者１２のユーザ名、及びそのユーザ名に関連付けられたパスワードのユーザ入力を受信するように構成される（ブロック２０４）。サーバ１８上で実行される認証アプリケーションは、ユーザ名とパスワードを検証するように構成される（ブロック２０６）。ユーザ名とパスワードが認証された場合、サーバ１８上で実行される認証アプリケーションは、典型的には、技術者１２によって選択される個人識別コード（ＰＩＣ）を促すように構成される（ブロック２０８）。いくつかの例示的な態様では、ＰＩＣは、認証アプリケーションによって生成され得る。サーバ１８は、入力されたＰＩＣを受信するように構成される。

【００３５】

サーバ１８上で実行される認証アプリケーションは、任意の好適な値であり得る有効期限値（例えば、有効期限日）を生成するように構成される（ブロック２１０）。例えば、有効期限値は、現在の時間／日後の所与の数の時間、日数、週間、又は月の場合であり得る。

【００３６】

サーバ１８上で実行される認証アプリケーションは、ユーザ名及び有効期限値、及び任意選択的にアクセス権（複数可）を含むログイン詳細のデジタル署名を生成するように構成される（ブロック２１２）。いくつかの例示的な態様では、サーバ１８上で実行される認証アプリケーションは、公開鍵基盤の秘密鍵に応答して（例えば、秘密鍵を含む証明書に基づいて）、技術者の雇用者などの認証団体のデジタル署名を生成するように構成される。

【００３７】

サーバ１８上で実行される認証アプリケーションは、ＰＩＣに基づくキーに応答して、有効期限値及び／又はユーザ名及び／又はデジタル署名及び／又はアクセス権（複数可）を（例えば、対称暗号化を使用して）暗号化するように構成される（ブロック２１４）。いくつかの例示的な態様では、有効期限値、ユーザ名、デジタル署名、及び任意選択的に

アクセス権（複数可）は、単一の項目として暗号化される。いくつかの例示的な態様では、有効期限値、ユーザ名、デジタル署名、及び任意選択的にアクセス権（複数可）は、個々に又は任意の好適な組み合わせで暗号化される。暗号化された有効期限値、ユーザ名、デジタル署名、及び任意選択的にアクセス権は、認証ファイル２８に記憶される。

【００３８】

サーバ１８上で実行される認証アプリケーションは、パスワードを認証したことに応答して（暗号化された有効期限値、パスワード、ログイン詳細のデジタル署名、及び任意選択的にアクセス権（複数可）を含む）認証ファイル２８をモバイルストレージデバイス２２に記憶するように構成される（ブロック２１６）。いくつかの例示的な態様では、サーバ１８上で実行される認証アプリケーションは、コンピューティングデバイス２４上で実行しているブラウザに認証ファイル２８を提供するように構成され、それにより、技術者１２は、認証ファイル２８をモバイルストレージデバイス２２に記憶するように選択することができる。

【００３９】

いくつかの例示的な態様では、有効期限値、及び／又はユーザ名、及び／又はデジタル署名は、モバイルストレージデバイス２２内の認証ファイル２８内に平文で記憶され得る。

【００４０】

ここで、図１のシステム１０内の認証ファイル２８を生成するために技術者１２によって使用されるユーザインターフェース画面３００の概略図である図３を参照する。ユーザインターフェース画面３００は、ユーザ名及びパスワードを入力するためのフィールド３０２、及びサーバ１８へのログインを要求するボタン３０４を含む。ユーザインターフェース画面３００は、ＰＩＣの入力を可能にするフィールド３０６、及び図２に記載されるように、認証ファイル２８の生成を要求するボタン３０８を含む。ダウンロードされた認証ファイル２８へのリンク３１０は、ユーザインターフェース画面３００の底部に示されており、これにより、技術者１２が、認証ファイル２８をモバイルストレージデバイス２２に記憶することが可能になる。

【００４１】

ここで、図１のシステム１０で使用するために認証ファイル２８が記憶されたモバイルストレージデバイス２２の概略図である図４を参照する。図示されるように、認証ファイル２８は、ＰＩＣに基づく鍵を使用する適切な暗号化アルゴリズムによって保護された（ブロック４０６）、有効期限値（ブロック４００）、ユーザ名（ブロック４０２）、デジタル署名（ブロック４０４）、及び任意選択的にアクセス権（複数可）を含む（ブロック４０８）。

【００４２】

ここで、認証ファイルを検証して、図１のシステム１０内のコンピューティングリソース１４へのアクセスを提供する方法における工程を含むフローチャート５００である図５を参照する。図１も参照されたい。

【００４３】

いったん認証ファイル２８又は関連値がモバイルストレージデバイス２２に記憶されると、技術者１２は、非接続処理デバイス１６のいずれかにモバイルストレージデバイス２２を取り込み得る。選択された非接続処理デバイス１６のうちの１つでは、技術者１２は、モバイルストレージデバイス２２を処理デバイス１６のデータインターフェース３０に動作可能に接続する。例えば、技術者１２は、モバイルストレージデバイス２２を処理デバイス１６のデータインターフェース３０に挿入する。処理回路３４上で実行される認証アプリケーションは、モバイルストレージデバイス２２に接続するように構成される（ブロック５０２）。

【００４４】

ここで、図１のシステム１０のコンピューティングリソース１４にログインするため技術者１２によって使用されるユーザインターフェース画面６００の概略図である図６を参

照する。処理回路３４上で実行される認証アプリケーションは、技術者１２がＰＩＣを入力するフィールド６０２と、モバイルストレージデバイス２２に記憶された認証ファイル２８を開くことを要求するボタン６０４と、を含むユーザインターフェース画面６００を表示デバイス上に提示するように構成される。技術者１２は、ユーザインターフェース画面６００にＰＩＣを入力し、モバイルストレージデバイス２２に記憶された認証ファイル２８を開くことを要求する。

【００４５】

再び図１及び図５を参照する。処理回路３４上で実行される認証アプリケーションは、ユーザ入力デバイス３２を介して、ＰＩＣ及び認証ファイル２８を開く要求のユーザ入力を受信するように構成されている（ブロック５０４）。処理回路３４上で実行される認証アプリケーションは、デジタル署名、有効期限値、ユーザ名、及び任意選択的に（暗号化形式で）アクセス権（複数可）を含む暗号化された認証ファイル２８を、モバイルストレージデバイス２２から受信するように構成される（ブロック５０６）。いくつかの例示的な態様では、処理回路３４上で実行される認証アプリケーションは、受信された個人識別コードに基づく鍵に応答して認証ファイル２８に含まれる以下のうちのいずれか１つ以上：有効期限値；ユーザ名；デジタル署名；及び任意選択的にアクセス権（複数可）、を対称復号化するように構成される（ブロック５０８）。

【００４６】

処理回路３４上で実行される認証アプリケーションは、有効期限値、ユーザ名、及び任意選択的にアクセス権（複数可）に応答してデジタル署名を検証し、有効期限値、ユーザ名、及び任意選択的にアクセス権（複数可）を認証するように構成される（ブロック５１０）。いくつかの例示的な態様では、処理回路３４は、公開鍵基盤の公開鍵に応答してデジタル署名を検証するように構成されている。

【００４７】

処理回路３４上で実行される認証アプリケーションは、有効期限値が期限切れでないことを確認するように構成される（ブロック５１２）。任意選択的に、処理回路３４は、ログイン詳細に含まれるアクセス権（複数可）（例えば、ユーザの許可、アクセスレベル、又は種類）を確認して、技術者が要求された機能にアクセスすることを認証されているかどうか、又は検証されたアクセス権（複数可）に基づいて機能を許可及び／又は解除するかを検証するように構成される。処理回路３４上で実行される認証アプリケーションは、（デジタル署名で）有効期限値とユーザ名が認証されていること、及び有効期限値が期限切れでないことに応答して、ユーザ名の下でログインされた（任意選択的に、検証されたアクセス権（複数可）に従って）コンピューティングリソース１４にアクセスを提供するように構成される（ブロック５１４）。デジタル署名の認証は、次に、正しい個人識別コードが、上述のように、技術者１２によって入力されて、認証ファイル２８を復号化するために使用されていることに依存する。

【００４８】

ここで、図１のシステム１０において使用するための認証ファイルを生成する別の方法における工程を含むフローチャート７００である図７を参照する。ブロック７０２～７１０の工程は、実質的に、図２を参照して上述したブロック２０２～２１０の工程に対応する。サーバ１８上で実行される認証アプリケーションは、入力された個人識別コード、ユーザ名、生成された有効期限値、及び任意選択的にアクセス権（複数可）を含むログイン詳細のデジタル署名を生成するように構成される（ブロック７１２）。サーバ１８上で実行される認証アプリケーションは、デジタル署名（典型的には、平文）、有効ファイル（典型的には、平文）、及びアクセス権（複数可）（典型的には、平文）を認証ファイルとしてモバイルストレージデバイス２２に記憶するように構成される（ブロック７１４）。

【００４９】

ここで、認証ファイルを検証して、図１のシステム１０内のコンピューティングリソース１４へのアクセスを提供するため別の方法における工程を含むフローチャート８００である図８を参照する。ブロック８０２～８０６の工程は、実質的に、図５を参照して上述

したブロック５０２～５０６の工程に対応する。
【００５０】
処理回路３４上で実行される認証アプリケーションは、（モバイルストレージデバイス２２内の認証ファイルに記憶されている）有効期限値、（ブロック８０４の工程で任意選択的に、技術者１２によって入力される）ユーザ名、（ブロック８０４の工程で入力された）ＰＩＣ、及び任意選択的にアクセス権（複数可）に応答してデジタル署名を検証し（ブロック８０８）、有効期限値、ユーザ名、ＰＩＣ、及び任意選択的にアクセス権（複数可）を認証するように構成される。いくつかの例示的な態様では、処理回路３４は、公開鍵基盤の公開鍵に応答してデジタル署名を検証するように構成されている。
【００５１】
処理回路３４上で実行される認証アプリケーションは、（モバイルストレージデバイス２２内の認証ファイルに記憶された）有効期限値が期限切れでないことを確認するように構成される（ブロック８１０）。任意選択的に、処理回路３４は、ログイン詳細に含まれるアクセス権（複数可）（例えば、ユーザの許可、アクセスレベル、又は種類）を確認して、技術者が要求された機能にアクセスすることを認証されているかどうか、又は検証されたアクセス権（複数可）に基づいて機能を許可及び／又は解除するかを検証するように構成される。処理回路３４上で実行される認証アプリケーションは、有効期限値、ユーザ名、（デジタル署名で）ＰＩＣが認証されていること、及び有効期限値が期限切れでないことに応答して、ユーザ名の下でログインされた（任意選択的に、検証されたアクセス権（複数可）に従って）コンピューティングリソース１４にアクセスを提供するように構成される（ブロック８１２）。
【００５２】
ここで、図１のシステム１０で使用するためにより多くのデータを備えた認証ファイル２８が記憶された図４のモバイルストレージデバイス２２の概略図である図９を参照する。図９に示す認証ファイル２８は、他のデータ中のユーザ取り消しリスト９００及び／又は公開鍵リスト９０２を含み得る。
【００５３】
いくつかの例示的な態様では、認証ファイル２８はまた、取り消しされているが期限切れでない認証ファイル及び／又は取り消しされているが期限切れでない認証ファイルのユーザをリスト化するユーザ取り消しリスト９００も含み得る。例えば、Ｅｖｅ及びＭａｌｌｏｒｙなどの技術者は退職しているが、彼らのモバイルストレージデバイス２２上の認証ファイル２８は、更に数週間、依然として有効である。したがって、Ｅｖｅ及びＭａｌｌｏｒｙは、各自のモバイルストレージデバイス２２を使用してコンピューティングリソース１４に不正にアクセスすることができる。現在雇用されている技術者のＡｌｉｃｅが、この期間中に新しい認証ファイルを要求する場合、Ｅｖｅ及びＭａｌｌｏｒｙの両方をリスト化するユーザ取り消しリスト９００（例えば、彼らのために生成された期限切れでない認証ファイルの詳細などの電子メール、ユーザ名、及び／又は他の識別詳細など）を新しい認証ファイル２８に追加することができ、それにより、Ａｌｉｃｅが異なるデバイスにログインするときにユーザ取り消しリスト９００をそれぞれのデバイスにコピーすることができるため、ＥｖｅとＭａｌｌｏｒｙが彼らのデバイスにログインしようとすると、ＥｖｅとＭａｌｌｏｒｙはユーザ取り消しリストに基づいてブロックされる。したがって、認証ファイルを要求し、認証ファイルに基づいてデバイスにログインするプロセスの結果として、ユーザ取り消しリスト９００がデバイスにコピーされる。ユーザ取り消しリスト９００は認証ファイル２８に含まれており、デジタル署名（ブロック４０４）はまた、ユーザがデバイスにログインするときにユーザ取り消しリスト９００の真正性を確認することができるように、ユーザ取り消しリスト９００に（例えば、現在の秘密鍵で）デジタル署名する。
【００５４】
認証ファイル２８はまた、ユーザ取り消しリスト９００のバージョンを識別するバージョン識別情報９０４を含み得る。バージョン識別情報９０４は、図１０を参照してより詳

細に説明されるように、ユーザ取り消しリスト９００の最新バージョンを追跡するために使用されるバージョン番号及び／又は日付を含み得る。例えば、Ａｌｉｃｅが医療デバイスにログインすると、医療デバイスは、Ａｌｉｃｅの認証ファイル２８に含まれるユーザ取り消しリスト９００のバージョン識別情報９０４（例えば、日付）が、医療デバイスのメモリに記憶されたユーザ取り消しリストのバージョン識別情報よりも新しいかどうかを確認する。実際に新しい場合、医療デバイスは、記憶されたユーザ取り消しリストを、Ａｌｉｃｅの認証ファイルで発見されるリストに置き換える。

【００５５】

ユーザ取り消しリスト９００は、２要素認証システム１０内のデバイスに接続することがもはや認証されていないユーザ、例えば、コンピューティングリソース１４にサービスを提供する会社のためにもはや働いていない技術者のリストを含み得る。ユーザ取り消しリスト９００は、２要素認証システム１０内のデバイスに接続することがもはや認証されていないが、期限切れでない認証ファイル２８へのアクセスを依然として有するユーザのリストを含み得る。ユーザ取り消しリスト９００は、ユーザ、ユーザ名、ユーザの電子メールアドレス、及び／又は取り消しされたユーザに割り当てられた認証ファイル２８などの他の識別情報のリストを含み得る。

【００５６】

異なる非接続処理デバイスにおける各コンピューティングリソースに、署名を検証するための少なくとも１つの公開鍵などがロードされているが、公開鍵は期限切れであるか、又は秘密－公開鍵ペアが危険にさらされている場合がある。したがって、１つ以上の予備の秘密－公開鍵ペアを生成し、デバイス上に少なくとも１つの予備公開鍵をロードすることが重要である。しかしながら、これは、デバイスがネットワークを介して接続され得ないことがあるため、問題となる。新しい秘密鍵は、その公開鍵の片割れが現場内の全てのデバイスに分配されるまで使用することができないことに留意されたい。移行を容易にするために、以下でより詳細に説明するように、認証ファイル２８を使用して、予備公開鍵（複数可）を分配することができる。

【００５７】

したがって、いくつかの例示的な態様では、認証ファイル２８は、少なくとも１つの予備公開鍵も含み得る。例えば、Ａｌｉｃｅが、新しい認証ファイルを要求する場合、１つ以上の予備公開鍵を新しい認証ファイル２８に追加することができ、それにより、Ａｌｉｃｅが異なるデバイスにログインするとき、予備公開鍵（複数可）は、後で使用するためにそれぞれのデバイスにコピーされ得る。したがって、認証ファイルを要求し、認証ファイル２８に基づいてデバイスにログインするプロセスの結果として、予備公開鍵（複数可）がそのデバイスにコピーされる。予備公開鍵（複数可）は、認証ファイル２８に含まれ得、デジタル署名（ブロック４０４）はまた、ユーザがデバイスにログインするときに、予備公開鍵（複数可）の真正性を確認することができるように、（例えば、現在の秘密鍵で）予備公開鍵（複数可）にデジタル署名する。

【００５８】

認証ファイル２８はまた、公開鍵リスト９０２のバージョンを識別するバージョン識別情報９０６を含み得る。バージョン識別情報９０６は、図１０を参照してより詳細に説明されるように、公開鍵リスト９０２の最新バージョンを追跡するために使用されるバージョン番号及び／又は日付を含み得る。公開鍵リスト９０２は、例えば、現在使用されている公開鍵（例えば、ＰＫ１）が期限切れであるとき、又は現在使用されている公開鍵と関連付けられた秘密鍵が何かしら危険にさらされている場合、２要素認証システム１０における将来の使用のために確保される１つ以上の予備公開鍵（例えば、ＰＫ２）を含み得る。公開鍵リスト９０２はまた、現在使用されている公開鍵（例えば、ＰＫ１）を含み得る。例えば、Ａｌｉｃｅが医療デバイスにログインすると、医療デバイスは、Ａｌｉｃｅの認証ファイル２８に含まれる公開鍵リスト９０２のバージョン識別情報９０６（例えば、日付）が、医療デバイスのメモリに記憶された公開鍵リストのバージョン識別情報よりも新しいかどうかを確認する。実際に新しい場合、医療デバイスは、記憶された公開鍵リス

トを、Ａｌｉｃｅの認証ファイル２８で発見されるリストに置き換える。
【００５９】
デジタル署名（ブロック４０４）は、現在使用されている公開鍵（例えば、ＰＫ１）に応答して検証のために現在使用されている秘密鍵（例えば、ＰＫ１に対応する秘密鍵）を使用して、（例えば、サーバ１８及び／又はコンピューティングデバイス２４によって）生成され得、ログイン詳細（有効期限値（ブロック４００）、ユーザ名（ブロック４０２）、アクセス権（複数可）（ブロック４０８））、並びにユーザ取り消しリスト９００及び公開鍵リスト９０２のうちの１つ以上にデジタル署名する。したがって、認証ファイル２８を記憶するモバイルストレージデバイス２２は、ユーザ取り消しリスト９００、公開鍵リスト９０２、ユーザ取り消しリスト９００のバージョン識別情報９０４、及び／又は公開鍵リスト９０２のバージョン識別情報９０６のうちの１つ以上を記憶する。認証ファイル２８は、暗号化され得る（ブロック４０６）。
【００６０】
ここで、認証ファイル２８を検証して、コンピューティングリソース１４へのアクセスを提供し、図１のシステム１０における古いユーザ取り消しリスト及び／又は古い公開鍵リストを置き換える別の方法における工程を含むフローチャート１０００である図１０を参照する。
【００６１】
データインターフェース３０は、モバイルストレージデバイス２２に接続するように構成され（ブロック１００２）、モバイルストレージデバイス２２は、（ログイン詳細、ユーザ取り消しリスト９００、バージョン識別情報９０４、公開鍵リスト９０２（例えば、予備公開鍵ＰＫ２を含む）、及び／又はバージョン識別情報９０６のうちの１つ以上をデジタル署名する）デジタル署名（図９のブロック４０４）；ユーザ取り消しリスト９００；公開鍵リスト９０２；バージョン識別情報９０４；バージョン識別情報９０６；及びログイン詳細（有効期限値、ユーザ名、アクセス権など）のうちの１つ以上を記憶する。
【００６２】
処理回路３４は、ユーザ名及びＰＩＣなどのログインデータのユーザ入力を受信するように任意選択的に構成される（ブロック１００４）。処理回路３４は、モバイルストレージデバイス２２から、デジタル署名（ブロック４０４）；ユーザ取り消しリスト９００；公開鍵リスト９０２（予備公開鍵（複数可）、例えば、ＰＫ２を含む）；バージョン識別情報９０４；バージョン識別情報９０６；及び任意選択的にログイン詳細（ブロック１００６）のうちのいずれか１つ以上を受信するように構成される。
【００６３】
処理回路３４は、現在の公開鍵（例えば、ＰＫ１）を使用して、（認証ファイル２８のログイン詳細に含まれる、又はブロック１００４の工程でユーザによって入力される）ログインデータ；ユーザ取り消しリスト９００；公開鍵リスト９０２；バージョン識別情報９０４；バージョン識別情報９０６、のうちの１つ以上に応答して、受信されたデジタル署名を検証して、ログインデータ；公開鍵リスト９０２に含まれる予備公開鍵（複数可）；ユーザ取り消しリスト９００；バージョン識別情報９０４；及び／又はバージョン識別情報９０６（ブロック１００８）、のうちの１つ以上を認証するように構成される。処理回路３４は、例えば、認証ファイル２８の有効期限値が依然として有効であることを確認するために、図１～図８を参照して上述した他の確認を実行するように構成され得る（ブロック１０１０）。処理回路３４は、認証されたログインデータに応答してコンピューティングリソース１４のうちの１つへのアクセスを提供するように構成され（ブロック１０１２）、他の確認が実行される。
【００６４】
いくつかの例示的な態様では、処理回路３４は、認証されたユーザ取り消しリスト９００のバージョン識別情報９０４が、認証されたユーザ取り消しリスト９００が古いユーザ取り消しリストよりも新しいことを示すことに応答して、（現在アクセスされている処理デバイス１６によって記憶及び使用される）古いユーザ取り消しリストの使用を、（モバ

イルストレージデバイス２２の認証ファイル２８に記憶されている）認証されたユーザ取り消しリスト９００に置き換えるように構成される（ブロック１０１４）。いくつかの例示的な態様では、処理回路３４は、新しい公開鍵リスト９０２が古い公開鍵リストより新しいことを、新しい公開鍵リスト９０２のバージョン識別情報９０６が示すことに応答して、（現在アクセスされている処理デバイス１６によって記憶及び使用される）古い公開鍵リストの使用を、新しい公開鍵リスト９０２に置き換えるように構成される。古いユーザ取り消しリスト９００及び／又は古い公開鍵リスト９０２は、削除され得る、又は処理デバイス１６によって記憶され得るが、使用されないことに留意されたい。

【００６５】

処理デバイス１６内の処理回路３４は、認証されたユーザ取り消しリスト９００に応答して、コンピューティングリソース１４へのアクセスを拒否するように構成される（ブロック１０１６）。例えば、ユーザ取り消しリスト９００上のユーザが処理デバイス１６のコンピューティングリソース１４にアクセスしようとする場合、アクセスは拒否される。

【００６６】

処理デバイス１６内の処理回路３４は、予備公開鍵が認証されている（すなわち、公開鍵リスト９０２が認証されたとき）ことに応答して、予備公開鍵（例えば、ＰＫ２）で追加のデジタル署名（例えば、処理デバイス１６への異なるログの場合）を検証するように構成される（ブロック１０１８）。

【００６７】

いったん全ての非接続デバイス１６が新しい公開鍵（複数可）を学習すると、新しい認証ファイル２８が新しい公開鍵の秘密鍵で署名され得る。その後、認証ファイル２８に記憶された公開鍵リスト９０２は、古い公開鍵を含む必要はなく、最終的には、全ての非接続デバイス１６は、公開鍵リスト９０２がそれらのデバイス１６において置き換えられるときに古い公開鍵を忘れる。

【実施例】

【００６８】

実施例１：ユーザを認証する方法であって、ログイン詳細の有効期限値（４００）及びデジタル署名（４０４）を記憶するモバイルストレージデバイス（２２）に接続することであって、ログイン詳細が、少なくともユーザ名（４０２）及び有効期限値を含む、接続することと、モバイルストレージデバイスからデジタル署名及び有効期限値を受信することと、個人識別コードのユーザ入力を受信することと、有効期限値及びユーザ名に応答してデジタル署名を検証して、有効期限値及びユーザ名を認証することと、有効期限値が期限切れでないことを確認することと、有効期限値及びユーザ名が認証されていることと、有効期限値が期限切れでないことと、個人識別コードと、に応答してユーザ名の下でログインされたコンピューティングリソース（１４）へのアクセスを提供することと、を含む方法。

【００６９】

実施例２：ログイン詳細が、少なくとも１つのアクセス権を含み（４０８）、検証することが、有効期限値、ユーザ名、及び少なくとも１つのアクセス権に応答してデジタル署名を検証して、有効期限値、ユーザ名、及び少なくとも１つのアクセス権を認証することを含み、確認することが、少なくとも１つのアクセス権を確認して機能へのアクセスが認証されているかどうかを検証することを含み、アクセスを提供することが、検証された少なくとも１つのアクセス権に従って、コンピューティングリソースへのアクセスを提供することを含む、実施例１に記載の方法。

【００７０】

実施例３：モバイルストレージデバイスが、暗号化形式で有効期限値を記憶し、方法が、個人識別コードに応答して有効期限値を復号化することを更に含む、実施例１又は２に記載の方法。

【００７１】

実施例４：モバイルストレージデバイスが、ユーザ名を暗号化形式で記憶し、方法が、

個人識別コードに応答してユーザ名を復号化することを更に含む、実施例１～３のいずれか１つに記載の方法。

【００７２】

実施例５：モバイルストレージデバイスが、暗号化形式でデジタル署名を記憶し、方法が、個人識別コードに応答してデジタル署名を復号化することを更に含む、実施例１～４のいずれか１つに記載の方法。

【００７３】

実施例６：個人識別コードに応答して有効期限値、ユーザ名、及びデジタル署名のうちの少なくとも１つを対称復号化することを更に含む、実施例１～５のいずれか１つに記載の方法。

【００７４】

実施例７：デジタル署名が、公開鍵基盤の秘密鍵及び公開鍵にそれぞれ応答して生成及び検証される、実施例１～６のいずれか１つに記載の方法。

【００７５】

実施例８：ユーザ名のユーザ入力を受信することと、有効期限値、ユーザ名、及び個人識別コードに応答してデジタル署名を検証して、有効期限値、ユーザ名、及び個人識別コードを認証することと、を更に含む、実施例１～７のいずれか１つに記載の方法。

【００７６】

実施例９：ウェブサーバをモバイルストレージデバイスに接続することと、ウェブサーバによってユーザ名、パスワード、及び個人識別コードのユーザ入力を受信することと、ウェブサーバによって有効期限値を生成することと、ログイン詳細のデジタル署名を生成することと、パスワードを認証したことに応答してログイン詳細の有効期限値及びデジタル署名をモバイルストレージデバイスに記憶することと、を更に含む、実施例１～８のいずれか１つに記載の方法。

【００７７】

実施例１０：個人識別コードに応答して有効期限値を暗号化することを更に含み、記憶することが、暗号化された有効期限値をモバイルストレージデバイスに記憶することを含む、実施例９に記載の方法。

【００７８】

実施例１１：個人識別コードに応答してユーザ名を暗号化することを更に含み、記憶することが、暗号化されたユーザ名をモバイルストレージデバイスに記憶することを含む、実施例９又は１０に記載の方法。

【００７９】

実施例１２：個人識別コードに応答してデジタル署名を暗号化することを更に含み、記憶することが、暗号化されたデジタル署名をモバイルストレージデバイスに記憶することを含む、実施例９～１１のいずれか１つに記載の方法。

【００８０】

実施例１３：ログイン詳細が、個人識別コードを含む、実施例９～１２のいずれかに記載の方法。

【００８１】

実施例１４：モバイルストレージデバイスが、ユーザ取り消しリストを記憶し、デジタル署名が、ログイン詳細及びユーザ取り消しリストにデジタル署名し、方法が、モバイルストレージデバイスからユーザ取り消しリストを受信することと、ユーザ取り消しリストに応答してデジタル署名を検証して、ユーザ取り消しリストを認証することと、認証されたユーザ取り消しリストに応答して、コンピューティングリソースへのアクセスを拒否することと、を更に含む、実施例１～１３のいずれか１つに記載の方法。

【００８２】

実施例１５：モバイルストレージデバイスが、ユーザ取り消しリストのバージョン識別情報を記憶し、方法が、認証されたユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証されたユーザ取り消しリストのバージョン識別情報が示すことに

応答して、古いユーザ取り消しリストの使用を認証されたユーザ取り消しリストに置き換えることを更に含む、実施例１４に記載の方法。

【００８３】

実施例１６：デジタル署名が、公開鍵基盤の第１の秘密鍵及び第１の公開鍵にそれぞれ応答して生成及び検証され、モバイルストレージデバイスが、第２の公開鍵を記憶し、デジタル署名が、ログイン詳細及び第２の公開鍵にデジタル署名し、方法が、モバイルストレージデバイスから第２の公開鍵を受信することと、第１の公開鍵に応答してデジタル署名を検証して、第２の公開鍵を認証することと、第２の公開鍵が認証されていることに応答して、第２の公開鍵で追加のデジタル署名を検証することと、を更に含む、実施例１～１５のいずれか１つに記載の方法。

【００８４】

実施例１７：モバイルストレージデバイスが、第１の公開鍵及び第２の公開鍵を含む新しい公開鍵リストと、新しい公開鍵リストのバージョン識別情報と、を記憶し、方法が、新しい公開鍵リストが古い公開鍵リストよりも新しいことを、新しい公開鍵リストのバージョン識別情報が示すことに応答して古い公開鍵リストの使用を新しい公開鍵リストに置き換えることを更に含む、実施例１６に記載の方法。

【００８５】

実施例１８：ユーザを認証する方法であって、ユーザ取り消しリスト（９００）と、ログイン詳細及びユーザ取り消しリストのデジタル署名（４０４）とを記憶する、モバイルストレージデバイス（２２）に接続することと、モバイルストレージデバイスからデジタル署名及びユーザ取り消しリストを受信することと、ユーザ取り消しリスト及びログインデータに応答してデジタル署名を検証して、ログイン詳細に含まれるユーザ取り消しリスト及びログインデータを認証することと、認証されたログインデータに応答して、コンピューティングリソース（１２）へのアクセスを提供することと、認証されたユーザ取り消しリストに応答して、コンピューティングリソースへのアクセスを拒否することと、を含む、方法。

【００８６】

実施例１９：モバイルストレージデバイスが、ユーザ取り消しリストのバージョン識別情報（９０４）を記憶し、方法が、認証されたユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証されたユーザ取り消しリストのバージョン識別情報が示すことに応答して、古いユーザ取り消しリストの使用を認証されたユーザ取り消しリストに置き換えることを更に含む、実施例１８に記載の方法。

【００８７】

実施例２０：ユーザを認証する方法であって、第１の公開鍵、第２の公開鍵に応答して検証のための第１の秘密鍵に応答して生成されたデジタル署名（４０４）を記憶するモバイルストレージデバイス（２２）に接続することであって、デジタル署名がログイン詳細及び第２の公開鍵にデジタル署名する、接続することと、モバイルストレージデバイスからデジタル署名及び第２の公開鍵を受信することと、第１の公開鍵に応答してデジタル署名を検証して、ログイン詳細に含まれる第２の公開鍵及びログインデータを認証することと、認証されたログインデータに応答して、コンピューティングリソース（１２）へのアクセスを提供することと、第２の公開鍵が認証されていることに応答して第２の公開鍵で追加のデジタル署名を検証することと、を含む、方法。

【００８８】

実施例２１：モバイルストレージデバイスが、第１の公開鍵及び第２の公開鍵を含む新しい公開鍵リスト（９０２）と、新しい公開鍵リストのバージョン識別情報（９０６）と、を記憶し、方法が、新しい公開鍵リストが古い公開鍵リストよりも新しいことを、新しい公開鍵リストのバージョン識別情報が示すことに応答して古い公開鍵リストの使用を新しい公開鍵リストに置き換えることを更に含む、実施例２０に記載の方法。

【００８９】

実施例２２：ユーザを認証するシステムであって、ログイン詳細の有効期限値（４００

）及びデジタル署名（４０４）を記憶するモバイルストレージデバイス（２２）に接続するように構成されたデータインターフェース（３０）を含む処理デバイス（１６）であって、ログイン詳細が、少なくともユーザ名（４０２）及び有効期限値を含む、処理デバイスと、ユーザ入力デバイス（３２）と、処理回路（３４）であって、モバイルストレージデバイスからデジタル署名及び有効期限値を受信し、ユーザ入力デバイスを介して、個人識別コードのユーザ入力を受信し、有効期限値及びユーザ名に応答してデジタル署名を検証して、有効期限値及びユーザ名を認証し、有効期限値が期限切れでないことを確認し、有効期限値及びユーザ名が認証されていることと、有効期限値が期限切れでないことと、個人識別コードと、に応答してユーザ名の下でログインされたコンピューティングリソース（１２）へのアクセスを提供するように構成された、処理回路と、

を備える、システム。

【００９０】

実施例２３：ログイン詳細が、少なくとも１つのアクセス権を含み（４０８）、処理回路が、有効期限値、ユーザ名、及び少なくとも１つのアクセス権に応答してデジタル署名を検証して、有効期限値、ユーザ名、及び少なくとも１つのアクセス権を認証し、少なくとも１つのアクセス権を確認して、機能へのアクセスが認証されているかどうかを検証し、検証された少なくとも１つのアクセス権に従って、コンピューティングリソースへのアクセスを提供するように構成されている、実施例２２に記載のシステム。

【００９１】

実施例２４：モバイルストレージデバイスが、暗号化形式で有効期限値を記憶するように構成され、処理回路が、個人識別コードに応答して有効期限値を復号化するように構成されている、実施例２２又は２３に記載のシステム。

【００９２】

実施例２５：モバイルストレージデバイスが、暗号化形式でユーザ名を記憶するように構成され、処理回路が、個人識別コードに応答してユーザ名を復号化するように構成されている、実施例２２～２４のいずれか１つに記載のシステム。

【００９３】

実施例２６：モバイルストレージデバイスが、暗号化形式でデジタル署名を記憶するように構成され、処理回路が、個人識別コードに応答してデジタル署名を復号化するように構成されている、実施例２２～２５のいずれか１つに記載のシステム。

【００９４】

実施例２７：処理回路が、個人識別コードに応答して有効期限値、ユーザ名、及びデジタル署名のうちの少なくとも１つを対称復号化するように構成されている、実施例２２～２６のいずれか１つに記載のシステム。

【００９５】

実施例２８：処理回路が、公開鍵基盤の公開鍵に応答してデジタル署名を検証するように構成されている、実施例２２～２７のいずれか１つに記載のシステム。

【００９６】

実施例２９：処理回路が、ユーザ名のユーザ入力を受信し、有効期限値、ユーザ名、及び個人識別コードに応答してデジタル署名を検証して、有効期限値、ユーザ名、及び個人識別コードを認証するように構成されている、実施例２２～２８のいずれか１つに記載のシステム。

【００９７】

実施例３０：モバイルストレージデバイスに接続し、ユーザ名、パスワード、及び個人識別コードのユーザ入力を受信し、有効期限値を生成し、ログイン詳細のデジタル署名を生成し、パスワードを認証したことに応答してログイン詳細の有効期限値及びデジタル署名をモバイルストレージデバイスに記憶する、ように構成されているサーバを更に備える、実施例２２～２９いずれか１つに記載のシステム。

【００９８】

実施例３１：サーバが、公開鍵基盤の秘密鍵に応答して、デジタル署名を生成するよう

に構成されている、実施例３０に記載のシステム。
【００９９】
実施例３２：サーバが、個人識別コードに応答して有効期限値を暗号化し、暗号化された有効期限値をモバイルストレージデバイスに記憶するように構成されている、実施例３０又は３１に記載のシステム。
【０１００】
実施例３３：サーバが、個人識別コードに応答してユーザ名を暗号化し、暗号化されたユーザ名をモバイルストレージデバイスに記憶するように構成されている、実施例３０～３２のいずれか１つに記載のシステム。
【０１０１】
実施例３４：サーバが、個人識別コードに応答してデジタル署名を暗号化し、暗号化されたデジタル署名をモバイルストレージデバイスに記憶するように構成されている、実施例３０～３３のいずれか１つに記載のシステム。
【０１０２】
実施例３５：ログイン詳細が、個人識別コードを含む、実施例３０～３４のいずれか１つに記載のシステム。
【０１０３】
実施例３６：モバイルストレージデバイスが、ユーザ取り消しリストを記憶し、デジタル署名が、ログイン詳細及びユーザ取り消しリストにデジタル署名し、処理回路が、モバイルストレージデバイスからユーザ取り消しリストを受信し、ユーザ取り消しリストに応答してデジタル署名を検証して、ユーザ取り消しリストを認証し、認証されたユーザ取り消しリストに応答して、コンピューティングリソースへのアクセスを拒否するように構成されている、実施例２２～３５のいずれか１つに記載のシステム。
【０１０４】
実施例３７：モバイルストレージデバイスが、ユーザ取り消しリストのバージョン識別情報を記憶し、処理回路が、認証されたユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証されたユーザ取り消しリストのバージョン識別情報が示すことに応答して、古いユーザ取り消しリストの使用を認証されたユーザ取り消しリストに置き換えるように構成されている、実施例３６に記載のシステム。
【０１０５】
実施例３８：デジタル署名が、公開鍵基盤の第１の秘密鍵及び第１の公開鍵にそれぞれ応答して生成及び検証され、モバイルストレージデバイスが、第２の公開鍵を記憶し、デジタル署名が、ログイン詳細及び第２の公開鍵にデジタル署名し、処理回路が、モバイルストレージデバイスから第２の公開鍵を受信し、第１の公開鍵に応答してデジタル署名を検証して、第２の公開鍵を認証し、第２の公開鍵が認証されていることに応答して、第２の公開鍵で追加のデジタル署名を検証するように構成されている、実施例２２～３７のいずれか１つに記載のシステム。
【０１０６】
実施例３９：モバイルストレージデバイスが、第１の公開鍵及び第２の公開鍵を含む新しい公開鍵リストと、新しい公開鍵リストのバージョン識別情報と、を記憶し、処理回路が、新しい公開鍵リストが古い公開鍵リストよりも新しいことを、新しい公開鍵リストのバージョン識別情報が示すことに応答して古い公開鍵リストの使用を新しい公開鍵リストに置き換えるように構成されている、実施例３８に記載のシステム。
【０１０７】
実施例４０：ユーザを認証するシステムであって、ユーザ取り消しリスト（９００）と、ログイン詳細及びユーザ取り消しリストにデジタル署名するデジタル署名（４０４）と、を記憶するモバイルストレージデバイス（２２）に接続するように構成されたデータインターフェース（３０）と、処理回路（３４）であって、モバイルストレージデバイスからデジタル署名及びユーザ取り消しリストを受信し、ユーザ取り消しリスト及びログインデータに応答してデジタル署名を検証して、ログイン詳細に含まれるユーザ取り消しリス

ト及びログインデータを認証し、認証されたログインデータに応答して、コンピューティングリソース（１２）へのアクセスを提供し、認証されたユーザ取り消しリストに応答して、コンピューティングリソースへのアクセスを拒否するように構成されている処理回路と、を備えるシステム。

【０１０８】

実施例４１：モバイルストレージデバイスが、ユーザ取り消しリストのバージョン識別情報（９０４）を記憶し、処理回路が、認証されたユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証されたユーザ取り消しリストのバージョン識別情報が示すことに応答して、古いユーザ取り消しリストの使用を認証されたユーザ取り消しリストに置き換えるように構成されている、実施例４０に記載のシステム。

【０１０９】

実施例４２：ユーザを認証するシステムであって、第１の公開鍵、第２の公開鍵に応答して検証のための第１の秘密鍵に応答して生成された、ログイン詳細及び第２の公開鍵にデジタル署名するデジタル署名（４０４）を記憶するモバイルストレージデバイス（２２）に接続するように構成されたデータインターフェース（３０）と、処理回路（３６）であって、モバイルストレージデバイスからデジタル署名及び第２の公開鍵を受信し、第１の公開鍵に応答してデジタル署名を検証して、ログイン詳細に含まれる第２の公開鍵及びログインデータを認証し、認証されたログインデータに応答してコンピューティングリソースへのアクセスを提供し、第２の公開鍵が認証されていることに応答して第２の公開鍵で追加のデジタル署名を検証するように構成されている、処理回路と、を備えるシステム。

【０１１０】

実施例４３：モバイルストレージデバイスが、第１の公開鍵及び第２の公開鍵を含む新しい公開鍵リスト（９０２）と、新しい公開鍵リストのバージョン識別情報（９０６）と、を記憶し、処理回路が、新しい公開鍵リストが古い公開鍵リストよりも新しいことを、新しい公開鍵リストのバージョン識別情報が示すことに応答して古い公開鍵リストの使用を新しい公開鍵リストに置き換えるように構成されている、実施例４２に記載のシステム。

【０１１１】

本開示の様々な特徴が、明確性のために別個の例示的な態様の文脈において記載されているが、これらが単一の例示的な態様に組み合わされて提供されてもよい。逆に、簡潔にするために単一の例示的な態様の文脈において記載されている本開示の様々な特徴が、別々に又は任意の好適な部分的組み合わせで提供されてもよい。

【０１１２】

上に述べた例示的な態様は例として挙げたものであり、本開示は上記に具体的に示し説明したものに限定されない。むしろ本開示の範囲は、上記の明細書で説明される様々な特徴の組み合わせ及びその部分的組み合わせの両方、並びに上述の説明を読むことで当業者に想到されるであろう、従来技術において開示されていないそれらの変形例及び修正例を含むものである。

【０１１３】

〔実施の態様〕

（１） ユーザを認証する方法であって、

ログイン詳細の有効期限値及びデジタル署名を記憶するモバイルストレージデバイスに接続することであって、前記ログイン詳細が、少なくともユーザ名及び前記有効期限値を含む、接続することと、

前記モバイルストレージデバイスから前記デジタル署名及び前記有効期限値を受信することと、

個人識別コードのユーザ入力を受信することと、

前記有効期限値及び前記ユーザ名に応答して前記デジタル署名を検証して、前記有効期限値及び前記ユーザ名を認証することと、

前記有効期限値が期限切れではないことを確認することと、
前記有効期限値及び前記ユーザ名が認証されていることと、前記有効期限値が期限切れではないことと、前記個人識別コードと、に応答して前記ユーザ名の下でログインされたコンピューティングリソースへのアクセスを提供することと、を含む方法。
（２） 前記ログイン詳細が、少なくとも１つのアクセス権を含み、
前記検証することが、前記有効期限値、前記ユーザ名、及び前記少なくとも１つのアクセス権に応答して前記デジタル署名を検証して、前記有効期限値、前記ユーザ名、及び前記少なくとも１つのアクセス権を認証することを含み、
前記確認することが、前記少なくとも１つのアクセス権を確認して、機能へのアクセスが認証されているかどうかを検証することを含み、
前記アクセスを提供することが、検証された前記少なくとも１つのアクセス権に従って、前記コンピューティングリソースへのアクセスを提供することを含む、実施態様１に記載の方法。
（３） 前記モバイルストレージデバイスが、暗号化形式で前記有効期限値を記憶し、前記方法が、前記個人識別コードに応答して前記有効期限値を復号化することを更に含む、実施態様１に記載の方法。
（４） 前記モバイルストレージデバイスが、前記ユーザ名を暗号化形式で記憶し、前記方法が、前記個人識別コードに応答して前記ユーザ名を復号化することを更に含む、実施態様３に記載の方法。
（５） 前記モバイルストレージデバイスが、暗号化形式で前記デジタル署名を記憶し、前記方法が、前記個人識別コードに応答して前記デジタル署名を復号化することを更に含む、実施態様１に記載の方法。
【０１１４】
（６） 前記個人識別コードに応答して前記有効期限値、前記ユーザ名、及び前記デジタル署名のうちの少なくとも１つを対称復号化することを更に含む、実施態様１に記載の方法。
（７） 前記デジタル署名が、公開鍵基盤の秘密鍵及び公開鍵にそれぞれ応答して生成及び検証される、実施態様１に記載の方法。
（８） 前記ユーザ名のユーザ入力を受信することと、
前記有効期限値、前記ユーザ名、及び前記個人識別コードに応答して前記デジタル署名を検証して、前記有効期限値、前記ユーザ名、及び前記個人識別コードを認証することと、を更に含む、実施態様１に記載の方法。
（９） ウェブサーバを前記モバイルストレージデバイスに接続することと、
前記ウェブサーバによって前記ユーザ名、パスワード、及び前記個人識別コードのユーザ入力を受信することと、
前記ウェブサーバによって前記有効期限値を生成することと、
前記ログイン詳細の前記デジタル署名を生成することと、
前記パスワードを認証したことに応答して前記ログイン詳細の前記有効期限値及び前記デジタル署名を前記モバイルストレージデバイスに記憶することと、を更に含む、実施態様１に記載の方法。
（１０） 前記個人識別コードに応答して前記有効期限値を暗号化することを更に含み、前記記憶することが、暗号化された前記有効期限値を前記モバイルストレージデバイスに記憶することを含む、実施態様９に記載の方法。
【０１１５】
（１１） 前記個人識別コードに応答して前記ユーザ名を暗号化することを更に含み、前記記憶することが、暗号化された前記ユーザ名を前記モバイルストレージデバイスに記憶することを含む、実施態様１０に記載の方法。
（１２） 前記個人識別コードに応答して前記デジタル署名を暗号化することを更に含み、前記記憶することが、暗号化された前記デジタル署名を前記モバイルストレージデバイスに記憶することを含む、実施態様９に記載の方法。

（１３）　前記ログイン詳細が、前記個人識別コードを含む、実施態様９に記載の方法。
（１４）　前記モバイルストレージデバイスが、ユーザ取り消しリストを記憶し、前記デジタル署名が、前記ログイン詳細及び前記ユーザ取り消しリストにデジタル署名し、前記方法が、
　前記モバイルストレージデバイスから前記ユーザ取り消しリストを受信することと、
　前記ユーザ取り消しリストに応答して前記デジタル署名を検証して、前記ユーザ取り消しリストを認証することと、
　認証された前記ユーザ取り消しリストに応答して前記コンピューティングリソースへのアクセスを拒否することと、を更に含む、実施態様１に記載の方法。
（１５）　前記モバイルストレージデバイスが、前記ユーザ取り消しリストのバージョン識別情報を記憶し、前記方法が、認証された前記ユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証された前記ユーザ取り消しリストの前記バージョン識別情報が示すことに応答して、前記古いユーザ取り消しリストの使用を認証された前記ユーザ取り消しリストに置き換えることを更に含む、実施態様１４に記載の方法。
【０１１６】
（１６）　前記デジタル署名が、公開鍵基盤の第１の秘密鍵及び第１の公開鍵にそれぞれ応答して生成及び検証され、
　前記モバイルストレージデバイスが、第２の公開鍵を記憶し、前記デジタル署名が、前記ログイン詳細及び前記第２の公開鍵にデジタル署名し、前記方法が、
　前記モバイルストレージデバイスから前記第２の公開鍵を受信することと、
　前記第１の公開鍵に応答して前記デジタル署名を検証して、前記第２の公開鍵を認証することと、
　前記第２の公開鍵が認証されていることに応答して前記第２の公開鍵で追加のデジタル署名を検証することと、を更に含む、実施態様１に記載の方法。
（１７）　前記モバイルストレージデバイスが、前記第１の公開鍵及び前記第２の公開鍵を含む新しい公開鍵リストと、前記新しい公開鍵リストのバージョン識別情報と、を記憶し、前記方法が、前記新しい公開鍵リストが古い公開鍵リストよりも新しいことを、前記新しい公開鍵リストの前記バージョン識別情報が示すことに応答して、前記古い公開鍵リストの使用を前記新しい公開鍵リストに置き換えることを更に含む、実施態様１６に記載の方法。
（１８）　ユーザを認証する方法であって、
　ユーザ取り消しリストと、ログイン詳細及び前記ユーザ取り消しリストのデジタル署名とを記憶する、モバイルストレージデバイスに接続することと、
　前記モバイルストレージデバイスから前記デジタル署名及び前記ユーザ取り消しリストを受信することと、
　前記ユーザ取り消しリスト及びログインデータに応答して前記デジタル署名を検証して、前記ログイン詳細に含まれる前記ユーザ取り消しリスト及び前記ログインデータを認証することと、
　認証された前記ログインデータに応答してコンピューティングリソースへのアクセスを提供することと、
　認証された前記ユーザ取り消しリストに応答して前記コンピューティングリソースへのアクセスを拒否することと、を含む、方法。
（１９）　前記モバイルストレージデバイスが、前記ユーザ取り消しリストのバージョン識別情報を記憶し、前記方法が、認証された前記ユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証された前記ユーザ取り消しリストの前記バージョン識別情報が示すことに応答して、前記古いユーザ取り消しリストの使用を認証された前記ユーザ取り消しリストに置き換えることを更に含む、実施態様１８に記載の方法。
（２０）　ユーザを認証する方法であって、
　第１の公開鍵、第２の公開鍵に応答して検証のための第１の秘密鍵に応答して生成されたデジタル署名を記憶するモバイルストレージデバイスに接続することであって、前記デ

ジタル署名がログイン詳細及び前記第２の公開鍵にデジタル署名する、接続することと、
前記モバイルストレージデバイスから前記デジタル署名及び前記第２の公開鍵を受信することと、
前記第１の公開鍵に応答して前記デジタル署名を検証して、前記ログイン詳細に含まれる前記第２の公開鍵及びログインデータを認証することと、
認証された前記ログインデータに応答してコンピューティングリソースへのアクセスを提供することと、
前記第２の公開鍵が認証されていることに応答して前記第２の公開鍵で追加のデジタル署名を検証することと、を含む、方法。

【０１１７】

（２１）　前記モバイルストレージデバイスが、前記第１の公開鍵及び前記第２の公開鍵を含む新しい公開鍵リストと、前記新しい公開鍵リストのバージョン識別情報と、を記憶し、前記方法が、前記新しい公開鍵リストが古い公開鍵リストよりも新しいことを、前記新しい公開鍵リストの前記バージョン識別情報が示すことに応答して、前記古い公開鍵リストの使用を前記新しい公開鍵リストに置き換えることを更に含む、実施態様２０に記載の方法。

（２２）　処理デバイスを備えるユーザを認証するためのシステムであって、前記処理デバイスが、
ログイン詳細の有効期限値及びデジタル署名を記憶するモバイルストレージデバイスに接続するように構成されたデータインターフェースであって、前記ログイン詳細が、少なくともユーザ名及び前記有効期限値を含む、データインターフェースと、
ユーザ入力デバイスと、
処理回路であって、前記モバイルストレージデバイスから前記デジタル署名及び前記有効期限値を受信し、前記ユーザ入力デバイスを介して個人識別コードのユーザ入力を受信し、前記有効期限値及び前記ユーザ名に応答して前記デジタル署名を検証して、前記有効期限値及び前記ユーザ名を認証し、前記有効期限値が期限切れでないことを確認し、前記有効期限値及び前記ユーザ名が認証されていることと、前記有効期限値が期限切れでないことと、前記個人識別コードと、に応答して前記ユーザ名の下でログインされたコンピューティングリソースへのアクセスを提供する、
ように構成された、処理回路と、
を備える、システム。

（２３）　前記ログイン詳細が、少なくとも１つのアクセス権を含み、
前記処理回路が、
前記有効期限値、前記ユーザ名、及び前記少なくとも１つのアクセス権に応答して前記デジタル署名を検証して、前記有効期限値、前記ユーザ名、及び前記少なくとも１つのアクセス権を認証し、
前記少なくとも１つのアクセス権を確認して、機能へのアクセスが認証されているかどうかを検証し、
検証された前記少なくとも１つのアクセス権に従って、前記コンピューティングリソースへのアクセスを提供する
ように構成されている、実施態様２２に記載のシステム。

（２４）　前記モバイルストレージデバイスが、暗号化形式で前記有効期限値を記憶するように構成され、
前記処理回路が、前記個人識別コードに応答して前記有効期限値を復号化するように構成されている、実施態様２２に記載のシステム。

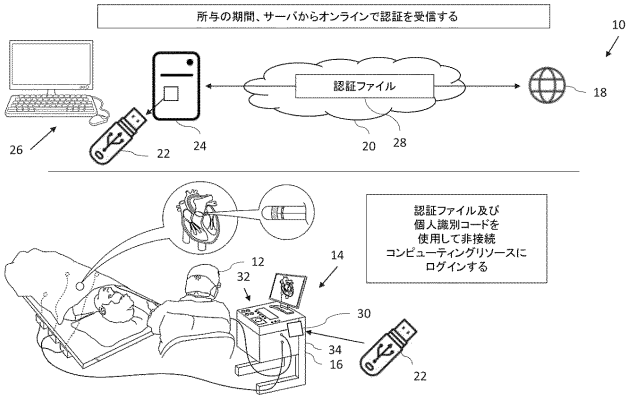
（２５）　前記モバイルストレージデバイスが、暗号化形式で前記ユーザ名を記憶するように構成され、
前記処理回路が、前記個人識別コードに応答して前記ユーザ名を復号化するように構成されている、実施態様２４に記載のシステム。

【０１１８】

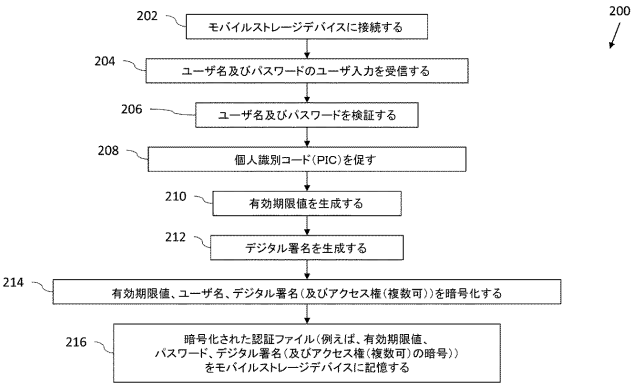
（２６）　前記モバイルストレージデバイスが、暗号化形式で前記デジタル署名を記憶するように構成され、
　前記処理回路が、前記個人識別コードに応答して前記デジタル署名を復号化するように構成されている、実施態様２２に記載のシステム。
（２７）　前記処理回路が、前記個人識別コードに応答して前記有効期限値、前記ユーザ名、及び前記デジタル署名のうちの少なくとも１つを対称復号化するように構成されている、実施態様２２に記載のシステム。
（２８）　前記処理回路が、公開鍵基盤の公開鍵に応答して前記デジタル署名を検証するように構成されている、実施態様２２に記載のシステム。
（２９）　前記処理回路が、
　前記ユーザ名のユーザ入力を受信し、
　前記有効期限値、前記ユーザ名、及び前記個人識別コードに応答して前記デジタル署名を検証して、前記有効期限値、前記ユーザ名、及び前記個人識別コードを認証する、
　ように構成されている、実施態様２２に記載のシステム。
（３０）　サーバを更に備え、前記サーバが、
　前記モバイルストレージデバイスに接続し、
　前記ユーザ名、パスワード、及び前記個人識別コードのユーザ入力を受信し、
　前記有効期限値を生成し、
　前記ログイン詳細の前記デジタル署名を生成し、
　前記パスワードを認証したことに応答して、前記ログイン詳細の前記有効期限値及び前記デジタル署名を前記モバイルストレージデバイスに記憶する、
　ように構成されている、実施態様２２に記載のシステム。
【０１１９】
（３１）　前記サーバが、公開鍵基盤の秘密鍵に応答して前記デジタル署名を生成するように構成されている、実施態様３０に記載のシステム。
（３２）　前記サーバが、
　前記個人識別コードに応答して前記有効期限値を暗号化し、
　暗号化された前記有効期限値を前記モバイルストレージデバイスに記憶する、
　ように構成されている、実施態様３０に記載のシステム。
（３３）　前記サーバが、
　前記個人識別コードに応答して前記ユーザ名を暗号化し、
　暗号化された前記ユーザ名を前記モバイルストレージデバイスに記憶する、
　ように構成されている、実施態様３２に記載のシステム。
（３４）　前記サーバが、
　前記個人識別コードに応答して前記デジタル署名を暗号化し、
　暗号化された前記デジタル署名を前記モバイルストレージデバイスに記憶する、
　ように構成されている、実施態様３０に記載のシステム。
（３５）　前記ログイン詳細が、前記個人識別コードを含む、実施態様３０に記載のシステム。
【０１２０】
（３６）　前記モバイルストレージデバイスが、ユーザ取り消しリストを記憶し、前記デジタル署名が、前記ログイン詳細及び前記ユーザ取り消しリストにデジタル署名し、
　前記処理回路が、
　前記モバイルストレージデバイスから前記ユーザ取り消しリストを受信し、
　前記ユーザ取り消しリストに応答して前記デジタル署名を検証して、前記ユーザ取り消しリストを認証し、
　認証された前記ユーザ取り消しリストに応答して前記コンピューティングリソースへのアクセスを拒否する、
　ように構成されている、実施態様２２に記載のシステム。
（３７）　前記モバイルストレージデバイスが、前記ユーザ取り消しリストのバージョン

識別情報を記憶し、
前記処理回路が、認証された前記ユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証された前記ユーザ取り消しリストの前記バージョン識別情報が示すことに応答して、前記古いユーザ取り消しリストの使用を認証された前記ユーザ取り消しリストに置き換えるように構成されている、実施態様３６に記載のシステム。
（３８） 前記デジタル署名が、公開鍵基盤の第１の秘密鍵及び第１の公開鍵にそれぞれ応答して生成及び検証され、
前記モバイルストレージデバイスが、第２の公開鍵を記憶し、前記デジタル署名が、前記ログイン詳細及び前記第２の公開鍵にデジタル署名し、
前記処理回路が、
前記モバイルストレージデバイスから前記第２の公開鍵を受信し、
前記第１の公開鍵に応答して前記デジタル署名を検証して、前記第２の公開鍵を認証し、
前記第２の公開鍵が認証されていることに応答して前記第２の公開鍵で追加のデジタル署名を検証する
ように構成されている、実施態様２２に記載のシステム。
（３９） 前記モバイルストレージデバイスが、前記第１の公開鍵及び前記第２の公開鍵を含む新しい公開鍵リストと、前記新しい公開鍵リストのバージョン識別情報と、を記憶し、
前記処理回路が、前記新しい公開鍵リストが古い公開鍵リストより新しいことを、前記新しい公開鍵リストの前記バージョン識別情報が示すことに応答して、前記古い公開鍵リストの使用を前記新しい公開鍵リストに置き換えるように構成されている、実施態様３８に記載のシステム。
（４０） ユーザを認証するためのシステムであって、
ユーザ取り消しリストと、ログイン詳細及び前記ユーザ取り消しリストにデジタル署名するデジタル署名と、を記憶するモバイルストレージデバイスに接続するように構成されたデータインターフェースと、
処理回路であって、
前記モバイルストレージデバイスから前記デジタル署名及び前記ユーザ取り消しリストを受信し、
前記ユーザ取り消しリスト及びログインデータに応答して前記デジタル署名を検証して、前記ログイン詳細に含まれる前記ユーザ取り消しリスト及び前記ログインデータを認証し、
認証された前記ログインデータに応答してコンピューティングリソースへのアクセスを提供し、
認証された前記ユーザ取り消しリストに応答して前記コンピューティングリソースへのアクセスを拒否する
ように構成されている、処理回路と、
を備えるシステム。
【０１２１】
（４１） 前記モバイルストレージデバイスが、前記ユーザ取り消しリストのバージョン識別情報を記憶し、
前記処理回路が、認証された前記ユーザ取り消しリストが古いユーザ取り消しリストよりも新しいことを、認証された前記ユーザ取り消しリストの前記バージョン識別情報が示すことに応答して、前記古いユーザ取り消しリストの使用を認証された前記ユーザ取り消しリストに置き換えるように構成されている、実施態様４０に記載のシステム。
（４２） ユーザを認証するためのシステムであって、
第１の公開鍵、第２の公開鍵に応答して検証のための第１の秘密鍵に応答して生成されたデジタル署名を記憶するモバイルストレージデバイスに接続するように構成されたデータインターフェースであって、前記デジタル署名がログイン詳細及び前記第２の公開鍵に

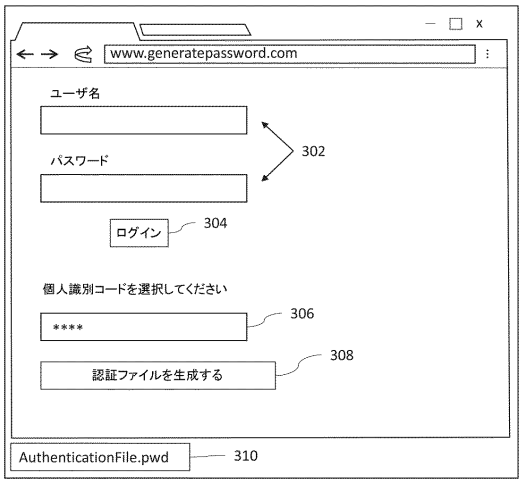
デジタル署名する、データインターフェースと、
処理回路であって、
前記モバイルストレージデバイスから前記デジタル署名及び前記第２の公開鍵を受信し、
前記第１の公開鍵に応答して前記デジタル署名を検証して、前記ログイン詳細に含まれる前記第２の公開鍵及びログインデータを認証し、
認証された前記ログインデータに応答してコンピューティングリソースへのアクセスを提供し、
前記第２の公開鍵が認証されていることに応答して前記第２の公開鍵で追加のデジタル署名を検証する
ように構成されている、処理回路と、
を備えるシステム。
（４３） 前記モバイルストレージデバイスが、前記第１の公開鍵及び前記第２の公開鍵を含む新しい公開鍵リストと、前記新しい公開鍵リストのバージョン識別情報と、を記憶し、
前記処理回路が、前記新しい公開鍵リストが古い公開鍵リストより新しいことを、前記新しい公開鍵リストの前記バージョン識別情報が示すことに応答して、前記古い公開鍵リストの使用を前記新しい公開鍵リストに置き換えるように構成されている、実施態様４２に記載のシステム。
【図面】
【図１】



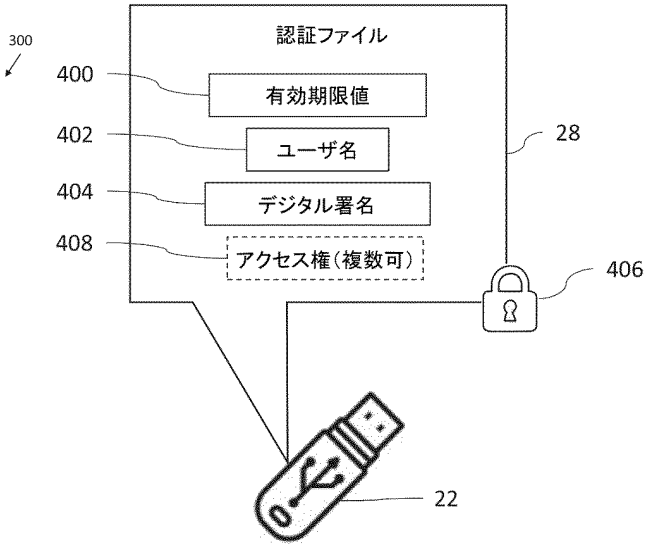
【図２】



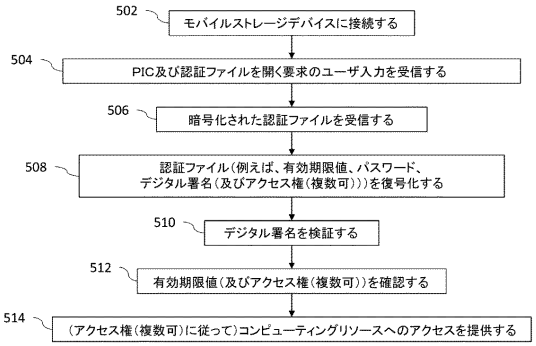
【図３】


www.generatepassword.com
ユーザ名
パスワード
302
ログイン
304
個人識別コードを選択してください
****
306
認証ファイルを生成する
308
AuthenticationFile.pwd
310

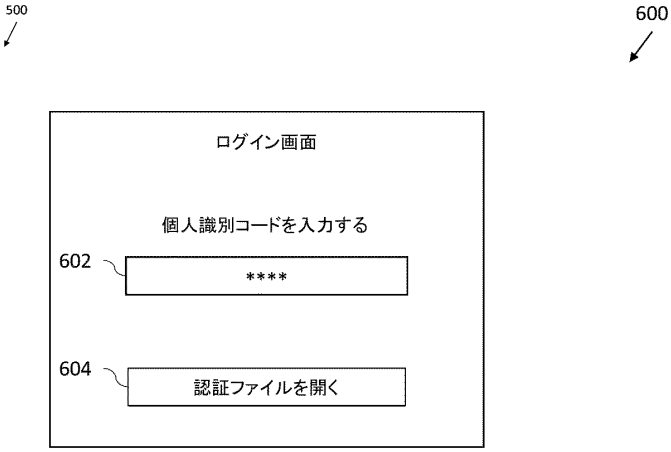
【図４】


300
認証ファイル
400
有効期限値
402
ユーザ名
404
デジタル署名
408
アクセス権（複数可）
28
406
22

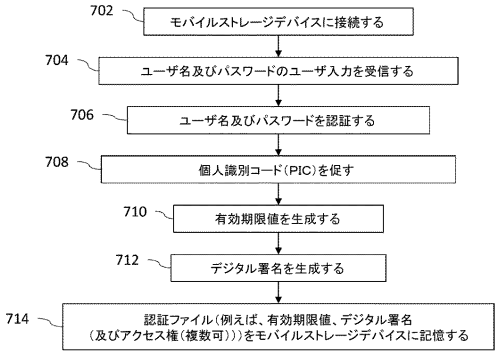
【図５】


502
モバイルストレージデバイスに接続する
504
PIC及び認証ファイルを開く要求のユーザ入力を受信する
506
暗号化された認証ファイルを受信する
508
認証ファイル（例えば、有効期限値、パスワード、
デジタル署名（及びアクセス権（複数可））を復号化する
510
デジタル署名を検証する
512
有効期限値（及びアクセス権（複数可））を確認する
514
（アクセス権（複数可）に従って）コンピューティングリソースへのアクセスを提供する

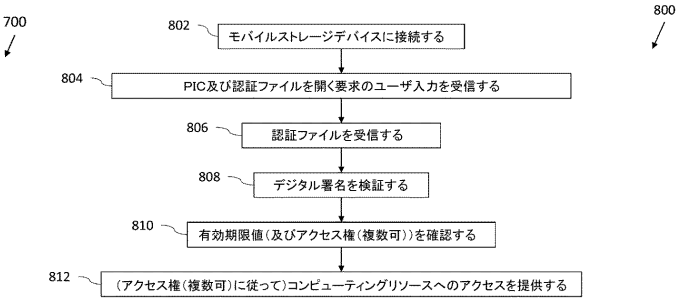
【図６】


500
600
ログイン画面
個人識別コードを入力する
602
****
604
認証ファイルを開く

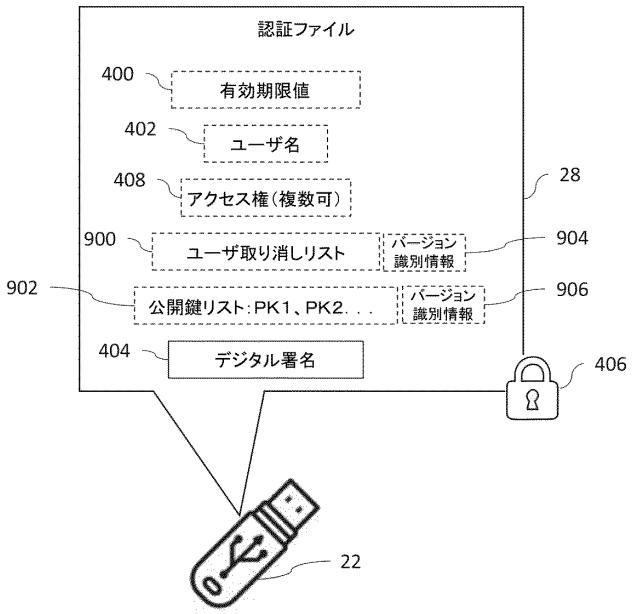
【図７】



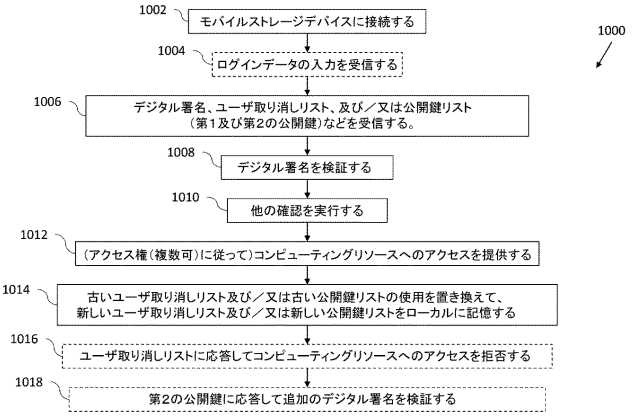
【図８】



【図９】



【図１０】



【外国語明細書】

2022162998000012.pdf

フロントページの続き

ンス・ウエブスター・（イスラエル）・リミテッド 気付け
(72)発明者 シュロモ・アム－シャレム
イスラエル国、２０６６７１７ ヨークナム、ハトヌファ・ストリート ４、ピー・オー・ボックス ２７５、バイオセンス・ウエブスター・（イスラエル）・リミテッド 気付け
(72)発明者 シュムエル・コーエン
イスラエル国、２０６６７１７ ヨークナム、ハトヌファ・ストリート ４、ピー・オー・ボックス ２７５、バイオセンス・ウエブスター・（イスラエル）・リミテッド 気付け
(72)発明者 フエ・グエン
アメリカ合衆国、９２６１８ カリフォルニア州、アーバイン、テクノロジー・ドライブ ３１、スイート・２００、バイオセンス・ウエブスター 気付け
(72)発明者 オー・ヤコボビッチ
イスラエル国、２０６６７１７ ヨークナム、ハトヌファ・ストリート ４、ピー・オー・ボックス ２７５、バイオセンス・ウエブスター・（イスラエル）・リミテッド 気付け